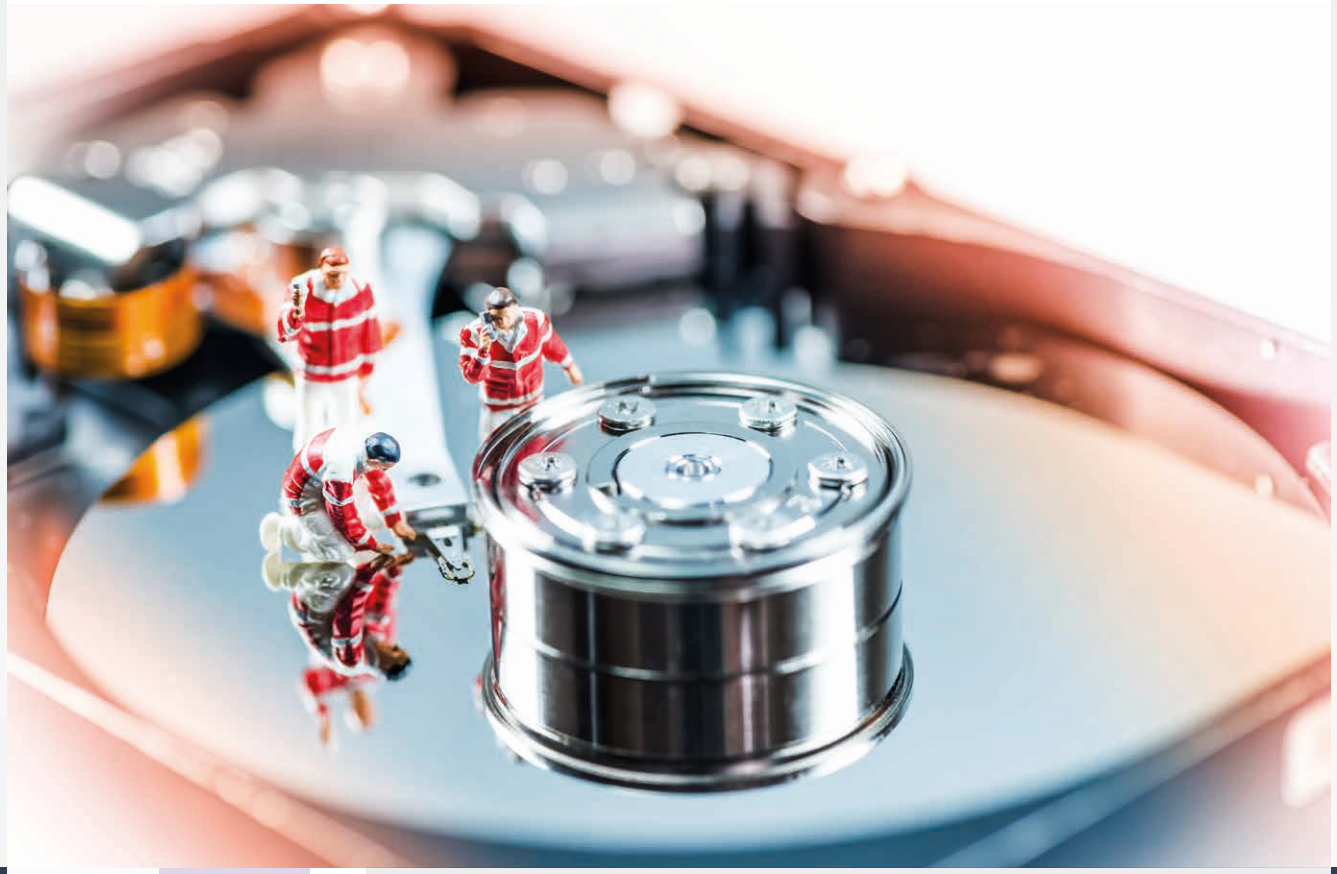
cam YOUR IT SOLUTIONS

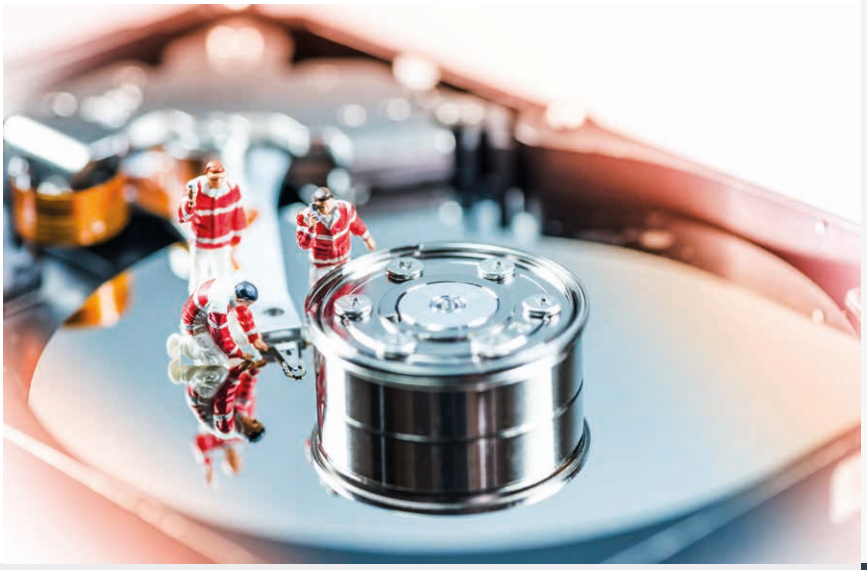
Voldoen aan de GDPR

Onderschat de rol van infrastructuur niet



Auteur: Rainier de Sitter, Chief Technology Officer Cam IT Solutions

Inhoudsopgave:



In het kader van GDPR kijken organisaties voornamelijk naar hun data en de applicaties. Toch speelt de infrastructuur ook een belangrijke rol in het compliant worden aan de nieuwe richtlijnen omtrent databeveiliging. Infrastructuurexpert Cam IT Solutions zet de verschillende aandachtspunten op een rij.

1. Inleiding

De komst van GDPR, die vanaf 25 mei 2018 zal worden gehandhaafd, dwingt organisaties tot het herijken van hun databeveiliging. Zorginstellingen zijn nu volop bezig om de status van hun datahuishouding in kaart te brengen. Welke data gaat er om in onze bedrijfsprocessen? Wat daarvan is privacygevoelig? Waar staat het?

Als een relatie bijvoorbeeld wil overstappen naar een andere ggz-instelling, kan hij eisen dat alle persoonlijke gegevens worden verwijderd. Dan moet de instelling of de ict-leverancier heel goed weten waar die data zich allemaal bevindt in de diverse systemen, in back-ups, in snapshots, in logs enzovoort.

Wie gebruikt de data en hoe doen zij dat? Hoe communiceer ik met mijn relaties – cliënten, medewerkers, patiënten, leveranciers – omtrent ons bezit en gebruik van hun privacygevoelige informatie? Hoe regel ik hun expliciete toestemming om die informatie te mogen gebruiken? Dit zijn de vragen waar zorginstellingen op dit moment volop mee bezig zijn.

> Zorginstellingen brengen momenteel de status van hun datahuishouding in kaart

Wanneer deze vragen zijn beantwoord, zal de focus zich verleggen naar vragen van een andere orde. Wat heb ik in mijn infrastructuur gedaan om datalekkage te voorkomen? Wat als er daadwerkelijk een datalek plaatsvindt? Hoe zijn wij daarop voorbereid? Kunnen we achterhalen wat er precies is gebeurd?

Zo is een van de onderdelen in de richtlijn dat een betrokkene moet worden geïnformeerd over de inbreuk, wanneer de inbreuk waarschijnlijk resulteert in een hoog risico voor haar/zijn rechten en vrijheden zodat zij/hij eventueel voorzorgsmaatregelen kan treffen. In sommige situaties kan dit via een openbare mededeling plaatsvinden, al is het ten zeerste de vraag of dat een gewenste handelswijze is…

Deze vragen bestrijken vele aspecten die een breed spectrum beslaan van bedrijfsprocessen tot de inrichting van ict-hulpmiddelen. Deze whitepaper beschrijft de maatregelen vanuit de ict-infrastructuur die bijdragen aan GDPR-compliancy.

Maar laten we eerst eens kijken wat de GDPR nu precies is.

2. Wat is GDPR/AVG?

De GDPR is ingesteld door de EU vanuit de noodzaak de bakens omtrent privacy van persoonsgegevens te verzetten. De digitalisering van onze maatschappij voltrekt zich in rap tempo, waar organisaties als Facebook, Instagram, Twitter, Amazon en Google dankbaar gebruik van maken. Nagenoeg ongestoord gebruiken zij de persoonsgebonden informatie voor marketingdoeleinden. GDPR betekent een nieuwe stap in het herkrijgen van onze privacy.

De afkorting staat voor General Data Protection Regulation. In het Nederlands hanteren we de term Algemene Verordening Gegevensbescherming (AVG). Met de Wbp (Wet bescherming persoonsgegevens) loopt Nederland voorop op de GDPR, waarin ook de Meldplicht datalekken is opgenomen. Deze meldplicht geldt in Nederland al sinds januari 2016. De GDPR is van kracht sinds april 2016, maar vanaf 25 mei 2018 zal de nog scherper geformuleerde verordening ook daadwerkelijk worden gehandhaafd.

Reputatieschade valt zelden in geld uit te drukken

Voor wie?
GDPR is van toepassing op zogeheten 'verwerkingsverantwoordelijken' en 'verwerkers' binnen de EU, en buiten de EU wanneer zij persoonsgegevens van EU-burgers verwerken. Onder die typische juridische term 'verwerkingsverantwoordelijken' verstaat de verordening: 'de organisatie die doel en methode van de gegevensverwerking bepaalt'. De 'verwerker' is dan 'de organisatie die de verwerking uitvoert namens en onder aanwijzing van de verwerkingsverantwoordelijke'.

Dat het de EU ernst is, blijkt wel uit de hoogte van de boetes die kunnen worden opgelegd. Onder de Wbp kan de Autoriteit Persoonsgegevens boetes tot en met € 820.000,- opleggen indien niet wordt voldaan aan de meldplicht datalekken. De boete wordt onder de GDPR een stuk hoger, oplopend tot € 20 miljoen of – indien dat hoger uitvalt – 4 procent van de jaarlijkse wereldwijde omzet per overtreding. Daar komt dan nog eens de reputatieschade bovenop, die zelden in geld valt uit te drukken.

Principes

Enkele principes van de algemene verordening gegevensbescherming zijn:

- Rechtmatige, behoorlijke en transparante verwerking. Ondernemingen moeten geldige redenen hebben om persoonsgegevens te verwerken en moeten de betrokkene hierover informeren.
- Doelbinding. De gegevens mogen alleen worden verwerkt voor het doel waarvoor de gegevens zijn verzameld.
- Instemming. De betrokkene moet over het algemeen instemmen met het verwerken van haar/zijn persoonsgegevens.
- Minimale gegevensverwerking. De verwerkte gegevens moeten beperkt zijn tot wat strikt noodzakelijk is voor een specifiek doel. Alleen degenen die de gegevens voor dat specifieke doel nodig hebben, krijgen toegang.
- Juistheid. De gegevens moeten juist zijn en onjuistheden moeten gemakkelijk kunnen worden gecorrigeerd. Een betrokkene heeft het recht om een dergelijke rectificatie te vragen.
- Opslagbeperking. De gegevens mogen alleen worden bewaard zolang ze noodzakelijk zijn voor het beoogde doel.
- Integriteit en vertrouwelijkheid. De gegevens moeten worden verwerkt onder adequate beveiliging, zodat ongeoorloofde verwerking en onopzettelijk verlies worden voorkomen.
- Verantwoordingsplicht. De onderneming moet in staat zijn de naleving van bovenstaande principes en gerelateerde corrigerende maatregelen aan te tonen. Een onderneming moet kunnen aantonen dat zij afdoende veiligheidsmaatregelen heeft genomen en dat naleving adequaat wordt gecontroleerd.

3. Anti-malware

Wat betreft GDPR heeft het in kaart brengen van de volledige datahuishouding momenteel de hoogste prioriteit bij zorginstellingen. Cam IT Solutions heeft daar, ogenschijnlijk, slechts zijdelings mee te maken. Dat komt omdat CAM zich voornamelijk bezighoudt met de applicaties die met data werken. De **CAM**CUBE is het infrastructuurplatform dat alle applicaties – van het EPD tot aan Microsoft Word – beschikbaar maakt en houdt. Toch zijn er diverse infrastructurele beveiligingsmaatregelen die helpen datalekken te voorkomen, en die eventuele 'nazorg' bij datalekken vergemakkelijken. Voor veel zorginstellingen is dit ongetwijfeld een 'volgende stap', maar ervaring leert dat die volgende stap vaak sneller gezet moet worden dan we denken.

> Diverse infrastructurele beveiligingsmaatregelen helpen datalekken voorkomen

Ransomware

Het proces naar een sterke GDPR-compliance is omvangrijk en tijdrovend, maar zeker niet onmogelijk. Een concrete beveiliging is het gebruik van anti-malwareoplossingen. Besmetting met ransomware waarbij persoonsgegevens zijn betrokken, wordt als een datalek gezien.

Nu is geen enkel systeem 100 procent veilig of ondoordringbaar. Helemaal niet wanneer gebruikers achteloos omspringen met de voorschriften. Zolang mensen hierin niet goed worden geïnstrueerd of de instructies worden bewust genegeerd, schiet iedere technische maatregel zijn doel voorbij. Maar aangezien de verantwoordelijkheid voor gegevensbescherming bij de organisatie ligt, en niet bij de eindgebruiker, is snelheid bij het detecteren van een lek essentieel.

Het is prachtig als de anti-malware een probleem detecteert en het direct de pas afsnijdt. Maar vaak wordt een probleem pas zichtbaar als het in werking treedt, bijvoorbeeld wanneer een systeem verbinding gaat leggen naar systemen, servers of databases waar het niets te zoeken heeft.

4. Segmentatie

Een belangrijke voorzorgsmaatregel is het segmenteren van het netwerk. Hiermee verhoog je niet alleen de detectiegraad, maar het ook de risicobeheersing. De schade van één besmette werkplek blijft beperkt, zeker in de werkwijze van de **CAM**CUBE waar geen data op een werkplek te vinden is.

De uitdaging wordt groter wanneer een virus horizontaal de organisatie ingaat naar filesystemen en databases. Segmentatie van het netwerk bemoeilijkt het verspreiden van malware. Bovendien kun je op die segmentatie IDS (Intrusion Detection System) toepassen, wat onverwachtse en ongewenste verbindingen heel snel detecteert.

Segmentatie helpt enerzijds om de impact van een eventuele breuk zoveel mogelijk te beperken. Anderzijds helpt het om lekken te voorkomen.

5. SIEM

Binnen de **CAM**CUBE worden alle logs centraal opgeslagen. Omdat ieder systeem wel een eigen log heeft, werden de logbestanden van oudsher sterk gedecentraliseerd bewaard. Het centraliseren van al die logs is op zich niet zo spannend, maar moet wel gebeuren. Dit vormt een goede voedingsbodem voor verdere analyse. Bij het vermoeden van een lek moet je achterhalen wat er precies heeft plaatsgevonden.

Zero-days

Centralisering van logs maakt deel uit van SIEM (Security Information & Event Monitoring), wat de beveiliging van systemen proactief aanpakt. Firewalls en anti-malwaredetectie werken reactief en hebben de beperking dat ze alleen eerder gedetecteerde malware eruit kunnen filteren. Zogeheten zero-days malware – een virus dat nog niet in de anti-virusdatabase staat – kan ongemerkt binnenkomen. In dat geval wordt een probleem pas zichtbaar als het in werking treedt. Daarom is SIEM zo belangrijk, omdat de analyse van logbestanden verdachte zaken kan opmerken, zoals het leggen van verbinding met ongewone servers in China of Rusland, of plotselinge hoge activiteit. Deze continue monitoring van systemen en analyse van logbestanden, maakt proactief en snel handelen bij mogelijke security issues veel gemakkelijker.

> SIEM pakt de beveiliging van systemen proactief aan

Analyse

Die analyse wordt steeds verder geautomatiseerd en is in dat opzicht al op indrukwekkende wijze geavanceerd, maar helemaal zonder mensenhanden en -ogen is het nog niet mogelijk. Om zero-days te ontdekken moeten correlaties worden gelegd tussen de logs, de activiteiten van systemen en de accounts. Doordat de systemen binnen de **CAM**CUBE 'met elkaar praten', wordt afwijkend gedrag heel snel herkend, wat de kans vergroot dat inbrekers in hun kraag worden gevat voordat ze iets hebben kunnen aanrichten.

Cam IT Solutions werkt nauw samen met cybersecurity specialist ON2IT, waar experts buiten de geautomatiseerde analyse om, de logs bekijken. Zij verrijken die logs om nog beter gedragsherkenning op hoog niveau toe te passen, zodat bedreigingen tijdig kunnen worden gedetecteerd.

Nu is geen enkele beveiliging waterdicht, dus mocht het toch misgaan, dan heb je met gecentraliseerde logs in ieder geval een gedetailleerde trail. Daarmee kan je volledig herleiden wat er is gebeurd. Bij het melden van een datalek kan je glashelder aangeven wat er is gebeurd, wat er is ontvreemd en welke tegenmaatregelen je hebt genomen.

72 uur

Als een verwerkingsverantwoordelijke een datalek opmerkt, moet hij dit meteen, waar mogelijk binnen 72 uur, melden aan de Autoriteit Persoonsgegevens. Daar komt heel veel bij kijken: het vermoeden van een lek, dit bevestigen, het bepalen van de impact van het lek, besluitvorming, inzet van resources (mensen, tooling). 72 uur zijn zo voorbij. Dus is het essentieel dat je een plan klaar hebt liggen, dat je kunt uitvoeren ingeval het nodig is.

Lukt het niet om het lek binnen 72 te melden, dan zal een verklaring gegeven moeten worden voor de vertraging. Dat betekent dat je snel een analyse op de logs moet kunnen doen, en dan moet je natuurlijk niet eerst nog eens die logs van overal en nergens vandaan moeten halen. Ook bij het bepalen van de impact van een datalek is snelheid geboden. Het kan zijn dat de betrokkenen moeten worden ingelicht over het feit dat hun persoonsgegevens zijn gelekt. Zij moeten namelijk de gelegenheid krijgen hun eigen maatregelen te treffen om schade zoveel mogelijk te beperken.

Herleiden

GDPR eist onder meer dat kan worden achterhaald of er een lek is geweest, en zo ja wat er uiteindelijk aan data is gecompromitteerd. Door de inrichting van de **CAM**CUBE en de centrale logging zie je snel of er ergens een stukje software is geïnstalleerd en welke connecties het met welke servers heeft opgebouwd, intern of extern. Zo kun je snel vaststellen of er iets aan data is gelekt, en zo ja, om welke data dat dan precies gaat.

Het is enorm belangrijk dat een organisatie bij het vermoeden van een lek niet eerst een dag gaat zitten nadenken van wat ze nu moeten doen. Ieder uur telt.

6. Toegangscontrole

Een ander aandachtspunt is toegangscontrole. Dat speelt een essentiële rol binnen de **CAM**CUBE. Zeker binnen de zorg is het niet vanzelfsprekend dat iedere werkplek snel en veilig beschikbaar is voor iedereen die achter het beeldscherm plaatsneemt. Een ziekenhuis heeft gemiddeld 500 verschillende applicaties, waar gebruikers diverse inlognamen en wachtwoorden voor moeten onthouden. In de praktijk worden wachtwoorden vergeten, wat de servicedesk belast. Of erger nog, ze staan op briefjes die onder het toetsenbord liggen.

> Wachtwoorden staan nog vaak op briefjes die onder het toetsenbord liggen

Met single sign-on behoort dit veiligheidsrisico tot het verleden. Onder één inlognaam en wachtwoord worden de namen en wachtwoorden van alle applicaties van een gebruiker veilig bewaard. Die ene inlognaam/wachtwoord ontsluit alle toepassingen die iemand mag gebruiken. Aan- en afmelden kan op iedere werkplek, zodat een inderhaast verlaten werkstation weinig tot geen risico op een datalek vormt.

De beveiligingseisen kunnen per werkplek worden ingesteld, zodat een werkplek in een publieke ruimte bijvoorbeeld alleen met tweefactor-authenticatie toegankelijk is.

7. Updaten/Patching

Het is wrang als we bedenken dat de meeste datagijzelingen met ransomware voorkomen hadden kunnen worden als er regelmatig updates van de diverse applicaties waren uitgevoerd. Naar schatting is 80 procent van de systemen in de zorg niet up-to-date. In een 24x7-organisatie als een ziekenhuis is dat ook een stevige uitdaging.

Hierin ligt ook een taak bij de leveranciers van applicaties. Zij kunnen hun software hoger beschikbaar maken, zodat die bijvoorbeeld voor de helft kan worden uitgezet voor de update, terwijl de andere 50 procent gewoon beschikbaar blijft.
CAM hanteert in haar infrastructuur een cadans waarbij updates elke drie maanden worden doorgevoerd, tenzij er uiteraard sprake is van een hoge urgentie, zoals met het WannaCry-virus.

Een andere oplossing is het virtueel patchen van systemen. Wanneer een bepaalde server operationeel is, kan die niet worden bijgewerkt. Wel is het mogelijk om de netwerkcomponent die staat voor die server te updaten.

En vergeet niet dat randapparatuur, zoals printers, scanners en dergelijke ook de oorzaak van een datalek kunnen zijn. Het geheugen van een printer kan vrij eenvoudig worden uitgelezen en als daar documenten met privacygevoelige informatie tussen zitten, kan dat nare gevolgen hebben.

8. Sandboxing

De klassieke anti-malware is gebaseerd op herkenning van bepaalde executables en dergelijke. Het leeuwendeel van alle malware – sommige bronnen spreken van 90 procent – komt in het veld maar één keer voor. De veranderingsgraad is dus zo hoog dat je er geen herkenning tegenaan kunt schrijven.

> De veranderingsgraad van malware is zo hoog dat herkenning nauwelijks mogelijk is

1 + 1 = 3

Daarom zijn de nieuwe anti-malwareproducten voor een belangrijk deel ingericht op gedragsherkenning. Om iets verdachts te detecteren, moeten alle security-onderdelen op elkaar zijn afgestemd. Je kunt het vergelijken met de beveiliging op een vliegveld. Wanneer een röntgenscanner – een van de security-onderdelen – een laag beveiligingsrisico detecteert, is dat op zich niet voldoende voor een stevige controle. Combineren we dat met andere observaties, zoals de ongebruikelijke route die iemand met een rugzak neemt, of de diverse korte gesprekken die hij met enkele personen heeft gevoerd, dan wordt één plus één drie. Op die manier kun je proactief verdachte zaken detecteren, dus voordat er iets gebeurt.

Zandbak

Wat er op deze manier aan verdachte datastromen wordt gedetecteerd, moet diepgaand worden geanalyseerd. Dit kan niet aan de interne kant van het netwerk worden gedaan. Dat zou de normale werkzaamheden onacceptabel vertragen. Hiervoor is sandboxing de ideale oplossing. Bestanden en executables die potentieel gevaarlijk zijn, komen automatisch in de sandbox terecht. In deze container wordt verdachte data geactiveerd. Is het malware dan richt het in die zandbak geen enkele schade aan. De bedreiging is ontmaskerd en wordt direct gemitigeerd, zodat het wereldwijd in beveiligingssystemen wordt bijgewerkt. Is het vals alarm, dan wordt de datastroom gewoon doorgestuurd.

9. Encryptie

In de preventieve sfeer is er nog encryptie, dat data die onderweg wordt afgevangen ontoegankelijk maakt. Hier zijn inmiddels vrij standaard oplossingen voor beschikbaar, al worden de controleslagen weliswaar steeds intensiever. Die race blijft natuurlijk gewoon doorgaan, en de encryptieniveaus worden voortdurend opgehoogd. Door regelmatig penetratietesten en kwetsbaarheidstesten uit te voeren, blijf je ook hier up-to-date.

Steeds meer digitaal verkeer is versleuteld. Wat voorheen aan de grenzen van een datacenter werd gedaan is steeds minder effectief. Er is een beweging waarneembaar naar het endpoint toe, of dat nu een server is of een werkplek.

10. Bewerkersverklaring

Ziekenhuizen en andere zorginstellingen zijn eigenaar van alle data. Als leverancier en beheerder van de infrastructuur hoeft CAM niets te doen met die data. CAM doet geen technisch applicatiebeheer, dus er vindt geen onderhoud plaats ín databases. Desondanks gaat de data over de hele infrastructuur heen, dus in die zin is ook CAM een trusted party. Daarom moet ook CAM de dataprivacy kunnen borgen. Hiertoe moet een zogeheten 'bewerkersverklaring' worden opgesteld, waaruit blijkt in hoeverre de ict-leverancier toegang heeft tot de data. Dat geldt ook voor andere ict-leveranciers, zoals Microsoft die Office 365 levert of leveranciers van cliëntendossierapplicaties die met name in de care vaak worden afgenomen als een dienst.

De nieuwe bewerkersverklaringen zullen in het licht van GDPR breder worden, of explicieter. Een en ander moet duidelijker worden aangegeven. Een leverancier als CAM kan niet langer volstaan met de verklaring dat het geleverde platform veilig is, zelfs niet wanneer dit onderbouwd wordt met NEN- en ISO-certificeringen. Ook CAM moet nu expliciet voor persoonsgegevens kunnen aantonen welke maatregelen zij wanneer op welke wijze hebben doorgevoerd.

11. Creëren van bewustzijn

Cam IT Solutions organiseert regelmatig architectuursessies. Ieder kwartaal bezoekt CAM haar relaties, waar – onder veel meer – ook over GDRP wordt gesproken. Dat is heel erg belangrijk, want heel vaak 'verzanden' deze bijeenkomsten in gesprekken over 'de waan van de dag': prestaties en beschikbaarheid van applicaties. Dat is logisch want over deze onderwerpen komt de meeste druk vanuit de organisatie. Maar het creëren van bewustzijn omtrent de nieuwe richtlijnen rondom gegevensbescherming, is essentieel om het ook te laten slagen.

> CAM biedt diverse mogelijkheden
> om te voldoen aan de GDRP-eisen

Veiligheid, bescherming van privacy, wordt van oudsher gezien als iets van ICT. Gelukkig verandert dat steeds meer, ook in de hogere managementlagen. Toch blijft het noodzakelijk dit steeds weer op tafel te leggen. De media helpen in dit opzicht ook mee, met hun berichtgeving over ransomware. Daarbovenop komt de dreiging van de extreme boetes waar de GDPR mee zwaait. Managers zijn hiervan echt onder de indruk.

Los daarvan, wil niemand dat zijn organisatie op de website van de Autoriteit Persoonsgegevens wordt vermeld in verband met een datalek. Cam IT Solutions biedt diverse mogelijkheden om te voldoen aan de GDRP-eisen. Onderschat in deze de rol van infrastructuur niet.

YOUR IT SOLUTIONS

Contact

Voor het voldoen aan de GDPR-richtlijnen is meer nodig dan alleen techniek. Toch verzorgt technische expertise zonder meer een gedegen basis voor adequate gegevens-bescherming.

Meer weten over infrastructurele tooling bij het bereiken van uw eigen GDPR-compliancy? Neem dan vrijblijvend contact op met de experts van Cam IT Solutions.

Cam IT Solutions B.V.
www.cam.nl
Edisonbaan 6
3439 MN Nieuwegein
T +31 (0)30 6005030