Algemene Verordening Gegevensbescherming (AVG)

We zijn inmiddels een tijdje verder sinds de invoering van de AVG en wat heb je hiervan gemerkt? Heb jij ook een lading aan e-mails gekregen met de vraag om akkoord te geven op de nieuwe voorwaarden?

Ondanks dat de overheid de wet Algemene Verordening Gegevensbescherming (AVG) per 25 mei handhaaft, denk ik dat veel bedrijven en organisaties nog niet AVG compliant zijn. Niet alleen organisatorisch maatregelen maar ook ICT technische maatregelen moeten genomen worden om aan deze wetgeving te voldoen.

De AVG is de Nederlandse naam voor de European General Data Protection Regulation (GDPR).

AVG focust zich op de bescherming van allerlei soorten van persoonsgegevens. Het kan gaan om de persoonsgegevens van klanten, patiënten en medewerkers. De AVG heeft ervoor gezorgd dat organisaties meer verantwoordelijkheden hebben gekregen omtrent het gebruik, opslaan en doorgeven van persoonsgegevens. Organisaties moeten voldoen aan de volgende punten:

- Transparantie: Organisaties moeten de personen informeren dat hun gegevens verwerkt worden. Daarnaast moet de organisatie de personen om toestemming vragen en hun rechten kenbaar maken.
- Doelbeperking: de persoonsgegevens worden voor een bepaald doel verzameld en mogen niet voor andere doeleinden gebruikt worden.
- Juistheid: De persoonsgegevens moeten correct zijn en blijven.
- Bewaarbeperking: De persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel.
- Integriteit en vertrouwelijkheid: De persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging
- Verantwoording: De bewerker van de persoonsgegevens moet kunnen aantonen dat het aan deze regels voldoet.

De AVG geeft de geregistreerde meer rechten zoals in de volgende punten beschreven:

- Recht op inzage: De persoon die geregistreerd is, heeft het recht om toegang te krijgen tot zijn/haar gegevens en het heeft recht op informatie over de manier waarop deze persoonsgegevens worden verwerkt.

- Recht op correctie en verwijdering: Een persoon heeft het recht om een verzoek in te dienen om de gegevens van die persoon te verwijderen of aan te passen.
- Recht op data portabiliteit: Een verwerker van persoonsgegevens dient, op verzoek van het individu, de gegevens over te dragen aan de door het individu voorgestelde partij.

Een groot aantal van de punten die in de AVG zijn opgenomen, zijn van procedurele aard. Het beschrijven van welke gegevens, hoe en hoelang je de persoonsgegevens bewaard en vooral waarom je de gegevens bewaard, is de basis waar je aan moet voldoen. Daarbij komen nog zaken zoals het bijhouden van een register van verwerkingsactiviteiten en voor bepaalde organisaties het aanstellen van een functionaris gegevensbescherming (FG). De meldplicht van een data lek aan de Autoriteit Persoonsgegevens bij gerede kans op schade voor de betrokkenen binnen de gestelde tijd van 72 uur was ook al van toepassing bij de wet Meldplicht Datalekken.

Een organisatie neemt een enorm risico als het geen processen heeft die aantonen dat ze de AVG als uitgangspunt hanteren bij het verwerken van persoonsgegevens. Ik zou als organisatie niet de case willen zijn voor de rechterlijke macht zodat ze eindelijk een jurisprudentie gaat opbouwen. Misschien is het nog meer bijzonder dat we nog geen rechtszaak hebben gehad inzake het lekken of verkeerd gebruik van persoonsgegevens. De hoogte van de boetes die in de wet zijn voorgeschreven zijn niet mals. Als deze ook werkelijk opgelegd gaan worden, is dat best een punt van aandacht. Dan kun je beter de 4% van jaaromzet of 20 miljoen Euro opnemen in je begroting voor AVG maatregelen.

Als het gaat om integriteit, vertrouwelijkheid en verantwoording zal een organisatie naast procedurele maatregelen toch ook technische maatregelen moeten hebben of alsnog maatregelen moeten nemen. Dit zijn dus de technische maatregelen om datalekken te voorkomen en naar mijn mening net zo belangrijk, te detecteren. Het nemen van preventieve maatregelen zal in de meeste gevallen niet het grootste probleem zijn. De maatregelen kun je realiseren met standaard ICT security componenten. De preventieve maatregelen stelt je bovendien in staat om te monitoren en acties te nemen op afwijkend gedrag. De preventieve maatregelen geven informatie over de handelingen van medewerkers, klanten en systemen. Het is verstandig om informatie te classificeren. De classificatie kun je relateren aan de bedrijfspolicy inzake verwerken van informatie. Maak eenvoudige spelregels die aangeven hoe je met informatie om moet gaan. De classificatie van informatie helpt hierbij. Met behulp van deze spelregels, kun je vervolgens bepalen welke technische maatregelen je moet nemen om je beleid te realiseren. Het beschrijven, bijhouden en toepassen van deze processen is met de invoering van AVG een belangrijk onderdeel geworden van de bedrijfsvoering. Enige vorm van certificering zoals ISO 27001 helpt hierbij.

Wat ik nog over deze certificeringen wil opmerken is dat veel mensen in bedrijven en organisaties, de certificeringsprocessen als die van de ISO 27001 als vervelend ervaren. Dat begrijp ik wel want er komt veel bij kijken. Maar er zit ook een andere kant aan en dat is dat je bewust bent van je eigen proces van informatie verwerken. Het is heel goed als de benodigde procedures ook gehandhaafd worden en dat je periodiek even in de spiegel kijkt of je het nog steeds goed doet. Het idee was toch immers dat je dit ooit hebt bedacht om fouten te voorkomen en efficiënt te werken?

Het zou best eens interessant kunnen zijn om een datalek te simuleren om te kijken of iedereen wel weet wat hij of zij moet doen. Het is een soort awareness training om collega's/medewerkers te confronteren met de praktijk.

DE PRAKTIJK VAN AVG MET ICT

Als Vosko kunnen we er niet voor zorgen dat jouw organisatie AVG compliant is of wordt. Maar we kunnen wel techniek leveren die jouw organisatie hierbij helpt. We kunnen naast de technische maatregelen ook de mensen leveren om deze technische maatregelen in te richten en te onderhouden.

Hierbij denk ik aan de volgende oplossingen:

Data Loss Prevention of Data Leakage Prevention (DLP)

DLP controleert de datastromen naar externe partijen op de policy waarin je bepaald welke informatie gedeeld mag worden met derden en op welke manier. DLP kan, als de policy wordt overtreden, ingrijpen met allerlei soorten van maatregelen. Je kunt DLP op de volgende manieren implementeren via:

- Email Security (Mail-Relay);
- Web proxy;
- Nex-Gen Firewall;
- Cloud Access Broker (CASB).

Voor alle DLP oplossingen geldt dat het samenstellen en bijhouden van de policy het meest belangrijke onderdeel is van de oplossing. Wij leveren de mensen die de oplossing bij je implementeren, onderhouden en de instellingen bijwerken.

Email Security (Mail-Relay)

Met behulp van een Email Security oplossing voor on-premise of in de cloud kun je DLP policies activeren voor email dataverkeer. De cloud oplossing die we kunnen bieden, integreert heel efficiënt met Office 365. Dit kunnen we je laten zien met een Proof of Concept. Het zou zomaar uit kunnen wijzen dat de standaard security oplossing in Microsoft Office 365 wel eens niet afdoende is voor je organisatie. We gaan graag de uitdaging aan om je dat te laten zien.

Web Proxy

Naast de email oplossing kunnen ook DLP activeren op een Web Proxy oplossing. Ook de proxy oplossing heeft zowel een on-premise als een cloud variant.
De combinatie van email en proxy geeft je al een heel duidelijk beeld van welke informatie naar het internet gaat en vanuit het internet binnenkomt.

Next-Gen Firewall

DLP functionaliteit kun je ook activeren op Next-Gen firewalls. Net als de Email Security en Web Proxy inspecteert het de datastromen die voorbij komen.

Cloud Security met Cloud Access Broker (CASB)

CASB zorgt ervoor dat je als organisatie de policies of rechtenstructuur die je in het interne netwerk hebt met betrekking tot documenten, rechten op shares en dergelijk, kunt doortrekken naar de cloud opslag en cloud applicaties zoals Microsoft OneDrive en Office 365 en Google Drive, Spark (of Webex Teams). De CASB oplossing biedt bovendien DLP functionaliteit zodat je de on-premise DLP policy ook kunt toepassen in de cloud. De DLP functionaliteit op proxy en mail-relay kijkt naar informatie ‘in transit’ of ‘in motion’. De CASB oplossing kijkt bovendien naar de informatie ‘in rest’.

De CASB oplossing geeft je de controle en zichtbaarheid terug die je helpt om in de cloud aantoonbaar in control te zijn.

Advanced Malware Protection

Voor AVG vind ik Advanced Malware Protection ook belangrijk. Veel informatie wordt gelekt door een besmetting met malware. Als je niet kunt aantonen dat je passende maatregelen hebt genomen als malware bescherming en detectie, heb je alsnog een probleem als er een lek is geconstateerd. Malware detectie gaat veel verder dan alleen antivirus software op de endpoints. De standaard antivirus, gebaseerd op signatures is vandaag de dag niet meer voldoende. Leveranciers van antivirus software voegen dan ook allerlei Next-Gen functionaliteit toe om de nieuwe ontwikkelde malware te kunnen detecteren en te blokkeren. Je ziet hierin een continue strijd tussen de hacker en de AV leveranciers.

De bescherming tegen malware kun je ook activeren op de firewall, mail-relay en proxy. Besmetting van malware kun je minimaliseren door een set aan maatregelen als antivirus, sandboxing, application control, IP reputation, DNS security en IPS. Ik ben zelf een groot voorstander van een gelaagde aanpak waarbij je op verschillende plaatsen bescherming aanbrengt tegen niet alleen malware maar ook andere aanvallen.

Netwerk Segmentatie

Netwerk segmentatie is het opdelen van je netwerk infrastructuur in logische delen. Met een Virtual LAN (VLAN) kun je een systeem of een groep systemen in een afgescheiden netwerkdeel plaatsen. Het segmenteren kun je toepassen omdat je het volgende wilt bereiken:

- Bij een virus uitbraak ben je in staat om delen van het netwerk te isoleren.
- Datatransport van het ene segment naar het andere segment wil je wel toestaan maar gecontroleerd door middel van een firewall.

Segmenteren kun je doen aan de hand van een aantal criteria. Het meest handige is om systemen, applicaties en informatie in te delen in security profielen bijvoorbeeld in een laag, midden en hoog security profiel niveau. Dit zorgt ervoor dat je niet per systeem hoeft te bepalen welke security maatregelen je moet nemen om het optimaal te beschermen.

Sterke of Multifactor Authenticatie en Role Bases Access

Als we toegang geven aan gebruikers geven tot informatie hoe weten we dan zeker dat we toegang gegeven hebben aan de juiste persoon? Een deel van dat vraagstuk lossen we op met sterke en multifactor authenticatie. We passen deze authenticatie vormen toe om gebruikers via een VPN tunnel toegang te geven tot de informatie intern. Door een gebruiker zich te laten authenticeren met niet alleen zijn userID en wachtwoord maar aanvullend een One-Time-Password op te laten geven die in een App op zijn telefoon wordt weergegeven, hebben we al meer zekerheid over zijn identiteit. Naast One-Time-Passwords zijn er nog een meer methoden om een gebruiker zijn identiteit te laten bevestigen. Zo kun je ook gebruik maken van push-notification, fingerprint of gezichtsherkenning.

Naast de authenticatie voor toegang, kunnen we met autorisatie bepalen waar een gebruiker toegang tot heeft. Met Role Based Access kunnen we toegangsregels per gebruik(sgroep) maken. Hierdoor voorkomen we dat we iedereen overal toegang tot geven.

Het afdwingen van sterke authenticatie en Role Based Access heeft als gevolg dat we van de acties van de gebruikers ook log meldingen kunnen krijgen. Dit geeft ons inzicht wie wat gedaan heeft en

op welk moment. Deze informatie kunnen we gebruiken bij een incident om te laten zien wat er gebeurt is.

Vulnerability Scanning

Het inzichtelijk maken van je kwetsbaarheden door middel van een vulnerability scan geeft je het inzicht in de kwetsbaarheden van de systemen en de infrastructuur. Het scannen van je infrastructuur heeft alleen zin als je aan de hand van de scan resultaten ook acties definieert als het installeren van patches op de kwetsbare systemen. Als je de segmentatie goed hebt doorgevoerd, zoals hiervoor is beschreven, weet je ook direct op welke systemen je als eerste moet focussen.

Web Application Firewall (WAF)

Waar ik mee wil afsluiten is de Web Application Firewall. Het beschermen van websites kan naar mijn mening veel beter. Toegang tot en het uitwisselen van informatie op web applicaties wordt veelal ongecontroleerd toegestaan. Als je bedenkt welke belangrijke informatie via portals binnenkomt of gedownload wordt, is het niet te verkopen dat dit ongecontroleerd gebeurt.

Met een Web Application Firewall (WAF) kun je de website beschermen tegen ongewenst gedrag van de bezoeker. Een goede WAF kan de website ‘leren’ waardoor het zelfs per invoerveld kan bepalen wat valide is. Het inrichten van een WAF is als je dit handmatig wilt doen best wel een hele klus. De betere WAF’s hebben tooling om de site te leren en een template te maken die je kunt toepassen om de website te beschermen.

Vraag: Heb je wel eens de hosting provider gevraagd van je website welke beschermingsmaatregelen ze genomen hebben om je website te beschermen?

Waarom ik deze vraag stel, is omdat ik in de praktijk vaak gezien heb dat web hosting providers geen enkele bescherming hebben opgenomen om de websites van hun klanten te beschermen. Je hebt bovendien als klant niet eens de mogelijkheid om de beschermlaag van een WAF toe te voegen. Tijdens het scannen van een website kon ik regelmatig ook met FTP inloggen of een pptp sessie opzetten. Al had ik geen account om in te loggen, het zijn allemaal mogelijkheden om een site plat te leggen.

Veel sites hebben een login button of link. Kun je het eens zijn met de volgende stelling: Elke site waar een login button of login link op staat moet voldoen aan de AVG /GDPR.

RESUMÉ

Om AVG-maatregelen te implementeren kun je de bestaande ICT technologie gebruiken om beschermings- en controlemaatregelen in realiseren. Met DLP, Threat Protection en een Web Application Firewall heb je al een heel aantal maatregelen, die je helpen om AVG compliant te zijn.

Naast de technische maatregelen zul je procedurele maatregelen nodig hebben om te kunnen voldoen aan de wetgeving. De procedures zijn mogelijk moeilijker in te richten dan de technische maatregelen die we je met de security componenten kunnen bieden. Het gaat bij procedures ook om een attitude verandering bij de medewerkers. Want medewerkers zijn de meest kwetsbare factor in een organisatie.

Maak een stappenplan om de maatregelen te implementeren om aan de AVG te voldoen zowel de procedures als de ICT maatregelen. Dat zorgt voor focus bij de organisatie die je nodig hebt om de maatregelen doelmatig in te richten.