Beveiligingsmogelijkheden Sharp

Sharp biedt uitgebreide beveiligingsmogelijkheden waarin oplossingen voor apparaatbeheer, output-beheer en documentenbeheer worden samengevoegd. Een belangrijk aspect van databeveiliging is de toegangs-verlening tot bepaalde data. Met een goede Data Security Kit is de MFP al beschermd tegen verschillende digitale aanvallen. Enerzijds gaat de beveiliging over de communicatie van en naar de printer toe, bijvoorbeeld op basis van IP- en MAC-adres filtering. Anderzijds is de informatie op de MFP die naar andere apparaten wordt gestuurd ook beveiligd. Dit gebeurt door middel van identificatie van de eigenaar van het document, maar het is ook mogelijk om scans te beveiligen met een wachtwoord.

Wat veel mensen niet weten is dat elke print-, scan- en kopieeropdracht van een MFP verloopt via of opgeslagen wordt op de interne harde schijf – die hierdoor een interessante bron van data is voor kwaad-willenden. Het is daarom bij Sharp ook mogelijk om de harde schijf te beveiligen met encryptie en aan het einde van het leasecontract de harde schijf plus alle instellingen volledig te wissen. Hierdoor voldoet de beveiliging van de MFP aan de AVG.

De bescherming van gevoelige documenten wordt een standaard dankzij de RSA encryptie van Adobe, het gebruik van SSL/TLS-protocollen en S/MIMME e-mail encryptie op de Sharp MFP. Een combinatie van software en de MFP helpt nog eens extra met de fysieke beveiliging van documenten, door te voorkomen dat fysieke documenten bij de verkeerde persoon terechtkomen doordat ze onbeheerd op de uitvoer van de MFP blijven liggen. De software op een MFP beschermt ook de documenten die op de printer zijn opgeslagen. De software zorgt namelijk voor het beheer van printopdrachten, zodat bepaalde documenten niet zomaar worden afgedrukt en in handen van derden kunnen komen. Iedere gebruiker heeft als het ware een eigen beveiligde persoonlijke omgeving in het documentbeheer, die alleen díe gebruiker kan inzien. Om het document af te drukken, moet de gebruiker zich eerst identificeren met bijvoorbeeld een toegangspas of een pincode. Hiermee wordt voorkomen dat personen toegang hebben tot documenten van anderen – waardoor er een potentieel datalek wordt voorkomen.

Het is geen enkel probleem om een MFP goed te beveiligen, maar dan moeten bedrijven hier wel een prioriteit van maken. Met betrekking tot de invoering van de AVG zijn bedrijven zich hier al steeds meer van bewust. Nu is het slechts een kwestie van het activeren van de beveiligingsmogelijkheden en het gebruiken van de juiste software.

Standaard bezit de Sharp MFP al een aantal features welke naar wens van de klant kunnen worden geactiveerd (niet voor iedereen noodzakelijk). Bijvoorbeeld een standaard firewall op de netwerkkaart. Als deze instelling geactiveerd is kan ingesteld worden welk netwerk device contact mag maken met de Sharp MFP en welke niet. Dit kan op IP of MAC niveau.

De data op de harddisk kan beveiligd worden door de standaard data security aan te zetten. Als de data security wordt aangezet, kan deze niet meer uitgezet worden! Na het activeren van deze functie wordt elke kopie, scan, print en fax versleuteld met 256 bit op de harddisk gezet. Na gebruik van data zal de ruimte die de data innam op de harddisk overschreven worden met variabele data zodat de originele data niet meer terug te halen is. Deze overschrijving kan ingesteld worden tussen 1 tot 10 maal overschrijving. Het instellen van data security kan alleen worden gedaan via de webpagina op de MFP zelf (zie plaatje).