EEN PARALLEL:

U BENT DE DATA, HET VLIEGTUIG IS UW WERKPLEK

Wanneer we het hebben over het beveiligen van uw omgeving, kunnen we dit uitstekend vergelijken met de beveiliging op een vliegveld. De veiligheidsmaatregelen op het vliegveld zijn iedereen wel bekend, maar hoe zorgt u er nu voor dat ook uw omgeving beschermd is tegen bedreigingen van buitenaf? Drie dingen: firewall, endpoint protection en spamfilter.

MARCEL PORTIER, TECHNISCH SPECIALIST

FIREWALL

De firewall opereert als een bescherming voor uw gehele netwerk en kan letterlijk gezien worden als een muur om uw netwerk. U kunt dit zien als de douanepoortjes die u op het vliegveld tegenkomt op weg naar de gate. U als reiziger bent de data, het gedeelte van de vluchthaven na de douane is uw netwerk, het vliegtuig is uw werkplek. Het meest veilige zou zijn om alle poorten continue dicht te houden, maar dat zou uw systeem niet-functioneel maken. Om met sommige internetdiensten te kunnen werken, zoals e-mail, is het nodig om bepaalde poorten open te zetten. Het is namelijk wel de bedoeling dat reizigers hun vlucht ook halen natuurlijk.
De firewall bevat een aantal modules die de beveiliging van uw netwerk optimaliseren, zoals een contentfilter, antivirussoftware of een Intrusion Prevention System (IPS). Een contentfilter voorkomt dat u onveilige websites bezoekt, antivirussoftware scant binnenkomende bestanden op mogelijke bedreigingen en een IPS houdt gevaarlijk verkeer bij de firewall tegen, bijvoorbeeld wanneer uw software beveiligingsrisico's heeft. U kunt deze modules zien als de marechaussee die altijd rondom de douane aanwezig is: de poorten zelf hebben niet de mogelijkheid gevaarlijke reizigers te weren, de marechaussee wel.

ENDPOINT PROTECTION

Waar de firewall bescherming biedt voor uw gehele netwerk, is de endpoint protection specifiek gericht op uw werkplek. Ook op het vliegveld doorloopt u bij de gate altijd een extra controle voordat u het vliegtuig in mag. Application control en antivirussoftware zijn de belangrijkste elementen van de endpoint protection. Sommige bedreigingen komen in de vorm van kwaadaardige software die zichzelf installeert in uw omgeving. Application control is software die dit tegenhoudt. Hiermee zet u enkel bekende en legitieme software op een 'whitelist', waarbij alleen deze programma's gestart kunnen worden. De vergelijking: de paspoort- en ticketcontrole. Alleen vakantiegangers met correct paspoort en ticket mogen boarden, anders worden ze tegengehouden. De antivirussoftware (extra marechaussee bij de gate) werkt als extra beveiliging na de firewall, een dubbelcheck als het ware.

SPAMFILTER

En tenslotte: de spamfilter. Een spamfilter is specifiek gericht op het opvangen, controleren en eventueel verwijderen van uw binnenkomende e-mail en staat daarom redelijk op zichzelf binnen uw beveiliging. In vliegveldterminologie: uw ruimbagage die gecontroleerd wordt voordat het aan boord van het vliegtuig gaat. Een specifiek type data dus, die vóór uw werkplek nog gecontroleerd wordt.

Zoals u ook veilig op het vliegtuig wilt stappen, wilt u natuurlijk ook dat uw omgeving beveiligd is. Uw beveiliging is echter, net als uw netwerk, op uw situatie afgestemd. Binnen deze drie elementen heeft u namelijk een legio aan mogelijkheden en gradaties, zodat u exact op een beveiliging kunt uitkomen die precies op uw behoeftes aansluit!

www.jds.nl