De meerwaarde van AI binnen een meerlaags informatiebeveiligingsmodel

Harm Teerenstra
Systems Engineer Public

Als publiek orgaan is de kans groot dat u zich in een spagaat bevindt; verdere digitalisering van data en processen nopen u tot de adoptie van moderne IT-middelen – denk aan het afnemen van applicaties vanuit een software-as-a-service model, het hosten van virtuele machines in de public cloud, of de implementatie van IoT-devices in het eigen netwerk – terwijl aan de andere kant wet- en regelgeving u verplicht er alles aan te doen de beschikbaarheid,integriteit en vertrouwelijkheid van data te borgen waardoor u wellicht liever afziet van dergelijke modernisering om zo meer zicht en grip te hebben op deze data. Binnen het speelveld van cybersecurity vinden echter ontwikkelingen plaats welke u juist in staat stellen eerstgenoemde evolutie met een gerust gevoel te omarmen zonder concessies te hoeven doen op het vlak van informatieveiligheid. Het kunnen creëren van een meerlaags informatiebeveiligingsmodel met naadloze out-of-the-box integratie tussen de verschillende oplossingen is één van deze ontwikkelingen, het gebruik van op artificiële intelligentie gestoelde technologie om de beveiligingseffectiviteit van deze oplossingen te verhogen is een andere. Fortinet – marktleider op het gebied van cybersecurity – zet sterk in op beide.

Meerlaags informatiebeveiligingsmodel

Eerdergenoemde digitalisering van data en processen leiden tot een verkaveling van de IT-infrastructuur, waarbij data zich op vele plaatsen bevindt. Ieder kavel – elk met een eigen perimeter – kent unieke risico's aangaande informatieveiligheid en dient dan ook op passende wijze beschermd te worden. Een veelvoorkomende valkuil is dat er vervolgens door een organisatie een beveiligingsarchitectuur wordt opgebouwd met diverse standalone securityoplossingen welke grotendeels onafhankelijk van elkaar functioneren. Hierdoor ontstaan silo's, met als gevolg een nagenoeg onbeheersbare omgeving en ineffectieve beveiliging.
Fortinet gelooft dat coherentie en integratie aan de basis dienen te staan van een efficiënte en effectieve securityarchitectuur. Vanuit deze visie heeft Fortinet diens cyber security platform ontwikkeld, genaamd Fortinet Security Fabric; hierbij werken producten/ oplossingen van Fortinet zelf, maar ook die van een brede groep technologiepartners, naadloos met elkaar samen. Als resultaat ontstaat een werkelijk geïntegreerde en coherente beveiligingsarchitectuur over alle lagen van de IT-infrastructuur heen.

Artificiële intelligentie

Met de oprichting van diens eigen threat researchafdeling FortiGuard Labs in 2005 heeft Fortinet breed ingezet op de adoptie van artificiële intelligentie om de beveiligingseffectiviteit van diens oplossingen toekomstbestendig te maken. Fortinet zag toen al dat securityoplossingen gestoeld op alleen signatures en/of definities op enig moment niet langer voldoende in staat zouden zijn de immer toenemende aanwas van nieuwe malware het hoofd te bieden. Middels machine learning technieken is het mogelijk gebleken heel nauwkeurig het betrouwbaarheidsniveau te bepalen van een bestand en/of generieke code, en op basis daarvan actie te ondernemen. Naast dat dit een bijzonder effectieve manier van malwarebestrijding bleek te zijn, nam tevens de mate van efficiëntie waarop threat intelligence kon worden gedeeld vanuit FortiGuard Labs toe door de kleinere footprint.

Door snel opeenvolgende ontwikkelingen in artificiële intelligentie zijn nu ook diverse oplossingen van Fortinet inmiddels zelf toegerust met machine learning technieken; te denken valt aan o.a. de Web Application Firewall (FortiWeb), de Advanced Threat Protection oplossing (FortiSandbox) en de Endpoint Detect & Respond oplossing (FortiEDR). Recentelijk is zelfs een virtuele SOC-analist beschikbaar gekomen in de vorm van FortiAI. Andere oplossingen binnen de Fortinet Security Fabric zullen volgen, maar profiteren te allen tijde reeds van de AI/ML-technieken die binnen FortiGuard Labs worden gehanteerd.

FORTINET®