FORTINET HEEFT TIEN JAAR ERVARING MET AI EN ML

Artificial intelligence en machine learning zetten cybersecurity kracht bij

Artificial intelligence (AI) en machine learning (ML) hebben de manier waarop we omgaan met technologie ingrijpend veranderd. Dat zal in de toekomst alleen maar toenemen, zegt Vincent Zeebregts, regional director Nederland bij Fortinet. Ook in het domein van cybersecurity maken AI en ML een opmars. “We willen onze partners daarom nieuwe perspectieven bieden op investeringen in security-oplossingen die door AI en ML worden ondersteund.”

Voor- en nadelen van artificial intelligence en machine learning

AI en ML spelen in de context van cybersecurity onder meer een rol bij het verwerken van enorme volumes aan malware, het detecteren van spam en misbruik van zakelijke e-mail, het inspecteren van netwerkverkeer, het gebruik van gezichtsherkenning, enzovoort. Machine learning houdt in dat computersystemen leren hoe ze een bepaalde taak moeten verrichten. Artificial intelligence wordt onder meer gebruikt voor een snelle analyse van grote datasets.

AI en ML ondersteunen het beslissingsproces en de bedrijfsprocessen. Maar ze zijn niet onfeilbaar. Elke AI- of ML-toepassing staat of valt met de informatie waarmee die is gevoed. Er zijn tal van voorbeelden te vinden van AI-algoritmes met ingebakken vooroordelen (bias), zoals de ‘fabeltjesfuik’ van Arjan Lubach. Toch kunnen AI en ML aanzienlijke voordelen bieden ten opzichte van nog veel feilbaardere mensen.

Vincent Zeebregts

Er wordt vaak gesproken van cybercriminelen die AI en ML inzetten voor de ontwikkeling van nieuwe malware. Toch is daar volgens Zeebregts weinig bewijs voor te vinden. “Cybercriminelen gebruiken AI en ML vooral om beveiligingsmechanismen te omzeilen. Denk bijvoorbeeld aan deep fake-video’s die mensen misleiden in het kader van phishing-trucs. AI en ML maken het ook mogelijk om captcha’s voor authenticatie te vervalsen en publiekelijk toegankelijke informatie over organisaties te verzamelen om gerichte aanvallen op specifieke gebruikers uit te voeren.”

AI en ML in de praktijk

De explosieve groei van malware, ransomware en andere cyberbedreigingen droeg in belangrijke mate bij aan de noodzaak van AI en ML. “Vroeger konden we de dagelijkse malware-volumes handmatig verwerken”, weet Zeebregts.

> **“Security-analisten kunnen hun werk niet doen zonder AI en ML”**

“Maar bijna van de ene op de andere dag groeide het aantal cyberaanvallen exponentieel. Security-analisten kunnen hun werk niet meer doen zonder AI en ML.”

Fortinet houdt zich al ruim tien jaar bezig met de inzet van AI en machine learning, vertelt Zeebregts. “Dat doen we op diverse fronten. Het begon met de introductie van de virtuele bedreigingsanalist van FortiGuard. Daarvoor ontwikkelden we een artificial neural network (ANN), dat malware-fragmenten in minder dan een seconde kan classificeren. Dit netwerk groeide na zes generaties uit tot FortiAI, dat miljoenen monsters per dag analyseert met een nauwkeurigheidspercentage van bijna 100%. Dit is een taak waarvoor normaliter duizenden menselijke analisten nodig zouden zijn.”

Het gebruik van ML bleek een goede manier te zijn om traditionele beveiligingsoplossingen kracht bij te zetten, vervolgt Zeebregts. “Denk bijvoorbeeld aan de toevoeging van door ML ondersteunde analyses aan FortiSandbox of FortiOS. Machine learning maakt tegenwoordig deel uit van nagenoeg al onze oplossingen, zoals FortiWeb en de FortiGuard Security Services. Daarmee helpen we onze klanten aan effectievere detectie van kwaadaardige activiteit en afwijkende patronen. Op dit gebied vormt innovatie de sleutel tot succes.”

AI en ML zijn volgens Zeebregts vooral goed in het blootleggen van verbanden en het doen van voorspellingen. “Ze kunnen bijvoorbeeld het DNA van twee malware-infecties vergelijken en de werkelijke oorzaak van beveiligingsproblemen achterhalen. Op basis van historische data en trendanalyses is het mogelijk om te voorspellen wat er binnen een netwerk gaat gebeuren.”

> **“Cybercriminelen gebruiken AI en ML vooral om beveiligingsmechanismen te omzeilen”**

Verschil tussen de oplossingen

De lessen die Fortinet in tien jaar tijd leerde over AI en ML worden toegepast binnen de Fortinet Security Fabric. “Wat de beveiliging op locatie betreft valt dan te denken aan inspectie van het internetverkeer, het verzamelen van relevante NOC-data en het gebruik van gezichtsherkenning”, zegt Zeebregts. “Wat beveiliging in de cloud betreft kan dit bijvoorbeeld gaan om het volgen van kwaadaardige internetcampagnes, detectie van zero day-bedreigingen en het trainen van neurale netwerken. Overigens worden niet alleen onze next-generation firewalls door ML ondersteund. Dat geldt voor ons complete beveiligingskader. De ervaring, innovaties en het onderscheidende vermogen van Fortinet vinden hun neerslag in deze uitgebreide, geïntegreerde en geautomatiseerde Security Fabric. Dat legt een solide basis voor de komende tien jaar, want we zijn vastbesloten om onze partners te ondersteunen met nog veel meer door AI en ML ondersteunde security-oplossingen.” ■