

# De risicomanager is te traag voor AI

Column van CFA Society Netherlands

**De gangbare wijze van cyber-risicobeheersing staat onder druk. Tijdsdruk welteverstaan. Want hoe wapen je je tegen de nieuwste generatie AI-modellen, die kwetsbaarheden steeds sneller kunnen vinden en uitbuiten?**

Wereldwijd waarschuwen financiële autoriteiten dit jaar opvallend eensgezind voor de cyberrisico's van de nieuwste generatie AI-modellen. En niet ten onrechte. Deze vooroplopende AI-modellen hebben inmiddels de capaciteiten om binnen een mum van tijd op autonome wijze kwetsbaarheden in veelgebruikte ICT-systemen en gedeelde infrastructuur te vinden en uit te buiten. Dat vormt een gevaar voor de stabiliteit van de financiële sector, aldus het Europees Comité voor Systeemrisico's.

Tegenover die technologische versnelling staat de traditionele risicobeheersing van financiële entiteiten. Die is juist ingericht op zorgvuldige afweging: kwetsbaarheden worden ieder afzonderlijk beoordeeld op ernst, kans op misbruik en mogelijke impact. Op basis van de hoogte van het risico worden vervolgens beveiligingsupdates getest en gecontroleerd uitgerold. Dat kost tijd en capaciteit, en vereist vaak betrokkenheid van externe leveranciers.

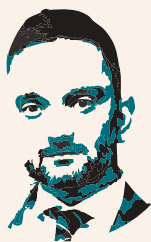
De huidige manier van werken komt onder druk te staan als aanvallers, gewapend met geavanceerde AI, fors meer kwetsbaarheden blootleggen. Dan ontstaan aan verdedigingszijde al snel capaciteitsproblemen, waardoor hoog-risico kwetsbaarheden mogelijk (te) laat worden aangepakt en lagere risico's misschien wel helemaal op de plank blijven liggen. Het huidige systeem dreigt het tempo niet meer bij te kunnen benen.

Wat doe je dan als risicomanager? De klassieke keuzes worden er niet aantrekkelijker op. Sneller updaten vergroot het risico op incidenten, uitgebreid blijven testen laat systemen langer kwetsbaar, en scherp prioriteren betekent dat andere zwakke plekken blijven liggen. Maar wat dan wel?

Een deel van het antwoord ligt eerder in de keten. De DORA-verordening verplicht financiële entiteiten al tijdens de ontwikkeling van ICT-systemen de beveiliging in te bedden en vóór ingebruikname grondig te testen. 'Secure by design' dus. Binnen die ontwikkelingscyclus kan AI volgens de Europese Commissie breed worden ingezet, bijvoorbeeld door code automatisch op beveiligingszwaktes te analyseren.

Het Agentschap van de Europese Unie voor Cyberbeveiliging (ENISA) roept daarnaast op de verdediging op te schalen naar 'machine-speed'. Dat betekent vergaande automatisering en inzet van AI in beveiligingsprocessen, bijvoorbeeld in de analyse en prioritering van kwetsbaarheden en de (bijna) onmiddellijke detectie van afwijkende activiteiten. Het doel is dat beveiligingsteams vrijwel direct kunnen reageren.

Dat is makkelijker gezegd dan gedaan. Opschaling naar dat niveau is voor veel (met name kleinere) partijen een grote uitdaging. Daarom blijft samenwerking onderling en met overheidsorganisaties van cruciaal belang. Ook toezichthouders spelen een belangrijke rol door nadrukkelijk te blijven toezien op naleving van de DORA-verordening en de Europese Cyberbeveiligingsverordening. Zonder 'machine-speed defence' is de risicomanager misschien te traag voor AI, maar hij staat er in ieder geval niet alleen voor. ■



Door **Can Yilmaz**,  
Regulatory & Compliance  
Consultant en lid van de  
Advocacy Committee van  
CFA Society Netherlands