Rijksoverheid

AI versnelt de dreiging *nu handelen is noodzakelijk*

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), het Nationaal Cyber Security Centrum (NCSC), de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), het Openbaar Ministerie (OM), CIO Rijk en de Nationale Politie zien dat Artificial Intelligence (AI) het dreigingslandschap significant verandert. AI versnelt dreigingen en het maakt het voor een bredere groep kwaadwillenden mogelijk om aanvallen uit te voeren. Kwetsbaarheden worden sneller opgespoord en misbruikt. Pijnpunten die al langer bestaan worden onder de invloed van AI uitvergroot. AI wordt ingezet door actoren om kwetsbaarheden te laten ontdekken én uitbuiten voordat de verdediger zich ergens van bewust is. Om hierop voorbereid te zijn is nu actie nodig.

We zien met regelmaat wat de gevolgen van cyberincidenten zijn als de verdediging niet op orde is: langdurige uitvallen van (vitale) systemen en veel burgers die slachtoffers zijn door tot het buitmaken van grote aantallen namen, adressen en BSN's met alle privacy en financiële consequenties tot gevolg. Daarnaast is de impact van cyberaanvallen soms niet direct zichtbaar. Statelijke actoren spioneren bij Nederlandse bedrijven, overheden en burgers en kunnen onopgemerkt gevoelige of geheime informatie buitmaken. Deze positie kan mogelijk gebruikt worden om in een later stadium schade aan te richten.

Daarom roepen wij bestuurders op hun verantwoordelijkheid te nemen en prioriteit te geven aan cybersecurity: stel de juiste middelen beschikbaar, prioriteer cybersecurity en geef experts de ruimte om de weerbaarheid van Nederland te verhogen.

Verandering van het dreigingslandschap

Cybersecurity is een strijd tussen aanval en verdediging. AI verlaagt de drempel voor aanvallers en maakt het voor een bredere groep kwaadwillenden mogelijk om cyberaanvallen uit te voeren. Kwetsbaarheden worden door AI steeds sneller opgespoord en misbruikt. Daardoor ontstaat er een nieuwe realiteit waar we ons aan moeten aanpassen.

Kwaadwillenden zetten AI vooral in om hun aanvalstechnieken te automatiseren, versnellen of efficiënter te maken: cyberaanvallen worden meer geavanceerd en blijven langer onder de radar. Ze kunnen met behulp van AI sneller aanvallen uitvoeren, makkelijker malware ontwikkelen, betere phishingmails schrijven en desinformatie op grote schaal personaliseren. Bovendien hoeven aanvallers geen gebruik te maken van de meest geavanceerde frontier modellen. Ook met het gebruik van bestaande en makkelijk toegankelijke AI-modellen kunnen dergelijke aanvallen nu al uitgevoerd worden.

Waarom dit vraagt om ander leiderschap

Digitale veiligheid is geen vraagstuk meer van alleen CISO's en IT'ers. De afhankelijkheid ervan is te groot, te complex en te risicovol voor organisaties. Het op orde brengen van de digitale weerbaarheid van ons land is een opdracht aan ons allen: publiek en privaat.

Om digitaal weerbaar te blijven is het noodzakelijk de risico's van AI mee te nemen in cybersecuritybeleid. Dit geldt voor de inzet van AI-modellen door kwaadwillenden, maar ook voor het gebruik van AI-modellen binnen jouw organisatie, zowel voor dagelijkse toepassingen als voor defensieve cybersecuritycapaciteiten.

Organisaties die hun basis op orde hebben, met prioriteit van hun bestuurders, met goed patchmanagement, een klein aanvalsoppervlak, logging en monitoring en inzicht in hun IT-landschap, staan in deze nieuwe realiteit aanzienlijk sterker.

De belangrijkste stap die we moeten zetten is niet technisch, maar cultureel en in de bewustwording. Cybersecurity is geen IT-probleem dat ergens in een kelder of datacenter opgelost wordt. Het is een breed organisatievraagstuk, een bestuursvraagstuk en uiteindelijk een maatschappelijk vraagstuk. We zijn zo sterk als onze zwakste schakel; en die zwakste schakel zit vaak niet in de techniek, maar in de bewustwording van het bestuur én de uitvoerders die zich onvoldoende bewust zijn van de cyberdreigingen.

Bestuurders nemen hun verantwoordelijkheid door eigenaar te zijn van de risico's en het beschikbaar stellen van de juiste (financiële) middelen.

Drie acties die bestuurders vandaag kunnen nemen om hun verantwoordelijkheid op te pakken:

1. De basis móet op orde

Geef in de bestuurskamers prioriteit aan cybersecurity. Het verkleinen van het aanvalsoppervlak en het vervangen van verouderde systemen die geen beveiligingsupdates meer krijgen is daarin een eerste stap. Stel middelen, zoals financiën, expertise en capaciteit, daarvoor beschikbaar. Het is niet te verantwoorden dat aanvallen kunnen plaatsvinden, omdat de basis niet op orde is en bijvoorbeeld patches niet of te laat worden geïnstalleerd. Juist nu de complexiteit in het dreigingsbeeld toeneemt, zijn basisprincipes een effectieve barrière. Je doet een autogordel niet om omdat de overheid dat voorschrijft, maar omdat je veilig wilt thuiskomen. Met de basismaatregelen is dat niet anders. De menselijke factor is daarin van groot belang: investeer in bewustwording, in gedrags- en cultuurverandering en doe aangifte bij incidenten. Techniek lost niet alles op: met de juiste cultuur en trainingen worden jouw medewerkers je sterkste verdediger.

2. Stel jezelf de vraag: Is mijn beveiliging nog op een passend niveau?

Zorg bijvoorbeeld voor adequaat patchmanagement zodat je beveiliging op niveau is. De race tussen het uitbrengen van patches en het misbruiken van kwetsbaarheden is niets nieuws, maar komt met laagdrempelige toegang tot AI-modellen wel in een stroomversnelling. Weken worden namelijk dagen en die dagen worden uren als het aankomt op updaten.

Bereid je daarom ook voor op het moment dat het toch misgaat. Dat is het principe van assume breach: ga ervan uit dat een aanvaller binnen kan komen en zorg dat je organisatie dan kan handelen. Wees voorbereid: weet wat je zelf kunt doen, waar je hulp bij nodig hebt en regel dat vooraf. Denk erover na, maak een plan en zorg dat medewerkers zijn opgeleid, getraind en geoefend om dat plan uit te voeren.

3. Neem signalen serieus

Volg ontwikkelingen op de voet en laat je adviseren door technische specialisten. In een toekomst waar AI een steeds grotere rol speelt voor zowel aanvallers als verdedigers, ligt het grootste risico niet bij AI maar bij jou, als bestuurder. Pas je daarom aan de nieuwe realiteit aan.

Onze gezamenlijke verantwoordelijkheid

De digitale weerbaarheid van Nederland staat in het kat-en-muis-spel tussen aanvallers en verdedigers altijd onder druk. AI-modellen versnellen dit proces en leggen de bestaande pijnpunten in onze digitale weerbaarheid nog duidelijker bloot.

Het cyberlandschap verandert door AI: cybercriminelen en statelijke actoren integreren het in hun strategie waardoor aanvallen sneller, complexer en grootschaliger worden. Zonder adequate reactie of voorbereiding op deze aanvallen, zoals de basis op orde, hebben toekomstige digitale aanvallen een grote impact op organisaties, sectoren en de samenleving.

Het voorkomen van beveiligingsincidenten zal voor elke organisatie een uitdaging blijven. Organisaties die zich goed voorbereiden, kunnen incidenten sneller detecteren en beheersen en de gevolgen voor de bedrijfsvoering en financiën beperken. Deze ontwikkelingen vragen daarom om verantwoordelijkheid van de overheid en bestuurders. Zij moeten de juiste beslissingen nemen en voldoende middelen beschikbaar stellen. Zo krijgen experts de ruimte om de cybersecurity in Nederland op orde te brengen. Alleen dan kunnen we de impact van digitale aanvallen en de dreiging op de samenleving zoveel mogelijk beperken.

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

AIVD
Simone Smit
Directeur-generaal

Ministerie van Defensie

MIVD
Peter Reesink
Vice-admiraal

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC
Matthijs van Amelsfort
Algemeen directeur

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

NCTV
Marc Kuipers
Nationaal Coördinator Terrorismebestrijding & Veiligheid

POLITIE

Politie
Janny Knol
Korpschef

OPENBAAR MINISTERIE

Openbaar Ministerie
Rinus Otte
Voorzitter College van procureurs-generaal

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

CIO Rijk
Art de Blaauw
CIO Rijk