



Europa staat op een kantelpunt in cybersecurity

'Al staat voor 'already infiltrated', vertelt CEO Rob Pike van Cyemptive. Traditionele detectie- en responsestrategieën zijn ontoereikend om AI-gedreven dreigingen het hoofd te bieden. De aanpak van Cyemptive – 'pre-emptive cyber defense' – voorkomt dat aanvallers überhaupt voet aan de grond krijgen.

CEO's moeten hun IT-cyberteam de vraag stellen of ze hun cybersecurity op orde hebben, stelt Pike. 'Als het antwoord 'ja' is, moet je je heel erg zorgen gaan maken. 'Nee' is een veel eerlijker antwoord, wanneer je je baseert op het beveiligingsniveau van dit moment.' Hij vervolgt: Zelfs als je AI-tools gebruikt om dreigingen van offensieve AI-systemen te detecteren, ben je eigenlijk altijd te laat.' De klanten van Cyemptive vervullen sleutelposities in de samenleving, zoals overheden, zorginstellingen, financiële instellingen, beheerders van kritieke infrastructuur en kennisinstituten en hoogwaardige industrieën. Het zijn stuk voor stuk organisaties die afhankelijk zijn van technologie die aanvallen autonoom kan voorkomen, voordat bedrijfsprocessen worden verstoord, gevoelige gegevens worden gestolen of vitale diensten uitvallen. De bestaande cybersecurityoplossingen die dreigingen detecteren nadat deze zich hebben voorgedaan schieten hierin tekort. 'Met AI-programma's als Claude is de mogelijkheid om kwetsbaarheden in coderingen te

ontdekken oneindig vermenigvuldigd. Die kun je bijna niet bijhouden. Daarom gebruiken we AI niet om te detecteren, maar als een 'back end'-device.'

Fundamenteel nieuwe benadering

Europa staat op een kantelpunt, door de schaduwoorlog met Rusland en de kracht van AI en kwantumcomputing. Europarlementariër Bart Groothuis waarschuwde onlangs voor een cyberbloedbad deze zomer. Pike: 'AI is een extreem disruptieve innovatie. Cybercriminelen kunnen dankzij AI met een ongekennde snelheid en schaal kwetsbaarheden identificeren, exploits ontwikkelen en systemen aanvallen.' Dit zorgt voor een fundamentele verandering van het cybersecuritylandschap, die een fundamenteel nieuwe benadering noodzakelijk maakt. Pike schetst een verontrustend beeld van de kwetsbaarheidsniveau. 'Onze specialisten komen regelmatig infiltraties in bedrijfssystemen tegen die al maandenlang gaande zijn. Als je met de informatie naar de CISO en zijn team gaat, en naar de

beveiliging vraagt, krijg je te horen dat alle signalen op groen staan. Terwijl de data onder hun ogen de deur uit vliegt!' Slechts 1% van de kwetsbaarheden is bekend, de overige 99% blijven onzichtbaar, volgens onderzoeksbureau Gartner. Deze schat dat de totale schade veroorzaakt door cybercrime inmiddels al is opgelopen tot 10 biljoen dollar op jaarbasis. Qua grootte zou het daarmee de derde economie ter wereld zijn. 'Als je cybersecurity zegt 'we doen het beter dan de

'Ons uitgangspunt luidt: de veiligste cyberaanval is de aanval die nooit plaatsvindt'

meesten', is het enige juiste antwoord: hoezo is dat relevant in een wereld waarin zelfs de grootste, meest gefocuste organisaties ter wereld worden geraakt? En te maken krijgen met een forse schade in reputatie en geld? Wat is je oplossing hiervoor?' Pike: 'Bij Cyemptive geloven wij dat cybersecurity moet evolueren van een reactieve naar een preventiegerichte aanpak. Het doel moet niet zijn om aanvallen te signaleren, dan ben je altijd te laat. Je moet zorgen dat aanvallen überhaupt niet succesvol kunnen worden uitgevoerd. De 'pre-emptive cyber defense' moet op orde zijn. Ons uitgangspunt luidt: de veiligste cyberaanval is de aanval die nooit plaatsvindt.' Het is een paradigmashift die nog onvoldoende wordt gemaakt. 'Cybersecurity moet veranderen van een reactieve naar een preventiegerichte aanpak. Daarvoor is het belangrijk om te begrijpen hoe aanvallers te werk gaan, verklaart hij. 'Als aanvallers eenmaal binnen zijn, willen ze zo lang mogelijk onopgemerkt in het systeem rondkijken en op onderzoek gaan naar data en kennis. En kijken hoe ze vaste voet aan de grond kunnen krijgen. Wat wij doen is de controle terugpakken, door aanvallers onschadelijk te maken voordat ze organisaties in het hart van hun bedrijfsvoering kunnen raken.'



Hoe zeker bent u of uw organisatie uw cybersecurity op orde heeft?
Scan de QR-code voor een kennismaking.