De verborgen kosten van goedkope software

Organisaties die digitale producten ontwikkelen, staan voortdurend onder druk om sneller en goedkoper te leveren. Neem je de beveiliging mee vanaf het begin of los je later op wat misgaat: dat dilemma keert steeds terug. Europese regelgeving zoals DORA en NIS2 maakt die keuze minder vrijblijvend. Persoonlijke aansprakelijkheid van bestuurders wordt hierdoor een juridische realiteit. Toch kiezen organisaties nog te vaak voor de schijnbaar goedkoopste route.

Jan Gerard Gerrits,
AI transformation director, Framna

Beveiliging krijgt bij digitale producten vaak pas aandacht in de backend. Bedrijven die zelf controle hebben over die backend, beperken beveiliging aan de voorkant soms tot een minimum. Maar zodra gevoelige informatie breder toegankelijk is dan nodig, neemt het risico op datalekken toe. Beveiliging goed inregelen vereist meer dan technische oplossingen: het is ook een operationeel vraagstuk dat specifieke kennis en ervaring vergt.

Sneller bouwen, groter risico

In de wereld van generatieve AI kan vrijwel iedereen software maken. Vibecoding heet het: binnen drie minuten een app ontwerpen en publiceren. Dat klinkt als vooruitgang, maar het heeft een keerzijde. De hoeveelheid middelmatige software groeit hierdoor snel, niet alleen qua productkwaliteit, maar ook qua beveiliging. “Zeker voor de hobbyist die beveiliging niet goed begrijpt, is het een best groot risico”, zegt Jan Gerard Gerrits, AI transformation director bij Framna. Het internationaal digitaal productbureau werkt voor organisaties in luchtvaart, financiële dienstverlening, zorg en kinderopvang. Voordat Gerrits zijn huidige rol aannam, was hij veertien jaar technisch directeur en security officer bij hetzelfde bedrijf.

Framna positioneert cybersecurity niet als los onderdeel van het ontwikkelproces, maar als productkenmerk. Beveiliging is verweven in elke fase: van ideevorming tot livegang en operationeel beheer. Dat begint in de designfase, voordat een technisch ontwerp wordt gemaakt. “De centrale vragen zijn dan: welke data verwerken we, moeten we die überhaupt verwerken, en hoe beveiligen we die in rust en tijdens overdracht?”, aldus Gerrits. “Vraag je altijd af: ‘Hebben we deze data écht nodig?’ Gevoelige persoonsgegevens moet je alleen verwerken als het strikt noodzakelijk is.”

Niet meer toegang dan nodig

Een van de meest voorkomende fouten die Gerrits tegenkomt, is het ontbreken van een least privilege-principe (alleen noodzakelijke toegang geven). Systemen en applicaties krijgen toegang tot meer informatie dan ze daadwerkelijk nodig hebben. Dat probleem speelt zowel op organisatorisch vlak als in de software zelf. “We krijgen weleens API’s aangeleverd van bedrijven waarvoor wij software maken. Dan kun je bijna door hun hele database grasduinen zonder dat dat nodig is. Scoping van informatieverstrekking is ontzettend belangrijk.”

> *Governance is een thema, maar de monitoring is minstens zo belangrijk*

Met de opkomst van AI-agents wordt dat principe nog urgenter. Een agent die toegang heeft tot meer data dan nodig, kan onbedoelde handelingen uitvoeren met gevoelige informatie. Governance speelt daarin een sleutelrol, maar Gerrits benadrukt dat het meer is dan beleid op papier. “Governance is een thema, maar de monitoring op wat er daadwerkelijk in het veld gebeurt, is minstens zo belangrijk.” Dat betekent investeren in observability: continu monitoren, automatische alerting bij verdacht gedrag en snelle detectie van penetratiepogingen.

Van bestuurskamer tot ontwikkelstraat

De invoering van DORA en NIS2 heeft cybersecurity hoger op de agenda gezet in bestuurskamers. Gerrits merkt dat uit eerste hand. “Ik kreeg plotseling allemaal DORA-agenda’s opgestuurd in de laatste maand voor de deadline. Omdat ik zelf in de directie zit, was security aan de bestuurstafel eigenlijk altijd al aanwezig. Maar ik kan me voorstellen dat het voor sommige bedrijven een must was vanuit NIS2, want anders blijft de verantwoordelijkheid worden afgeschoven op de security officer.”

Die structurele aanpak vertaalt zich naar de operationele kant. Na de ontwikkelfase volgen verplichte pentests voordat een product live gaat. In de operationele fase draait het om SIEM-oplossingen, continue observability en automatische alerting. “De snelheid van softwareontwikkeling gaat omhoog door AI, maar de ‘human judgement’ blijft onmisbaar. Alles wat gegenereerd wordt door AI, wordt altijd nog door vier ogen bekeken. AI kan nooit zelf iets live zetten”, benadrukt Gerrits.

Vertrouwen als concurrentievoordeel

Organisaties die cyberveiligheid serieus nemen, bouwen aan iets wat moeilijk te kopiëren is: een bewezen track record. Certificeringen zoals ISO en PCI-DSS, gecombineerd met aantoonbare ervaring bij veeleisende opdrachtgevers, maken het verschil wanneer een klant moet kiezen tussen aanbieders. “Iedereen zegt dat ze veilig zijn. Maar je moet een trusted partner zijn met een bewezen track record”, aldus Gerrits. Framna bereidt zich inmiddels voor op de nieuwe AI-ISO-standaard 42001, om ook op dat vlak de lat hoog te houden.

“Cybersecurity is voor ons een strategic enabler, geen blok aan ons been”, zegt Gerrits. “Digitale weerbaarheid is een verplichting geworden. En de mindset in het bedrijf is dat iedereen begrijpt wat onze security posture (beveiligingsstatus) is als we iets naar buiten brengen, dat is uiteindelijk waar het om draait.”