Veiliger innoveren

door: Mirjam Hulsebos

Datalekken, nieuw ontdekte kwetsbaarheden en aanvallen zijn dagelijks in het nieuws. Daarnaast kan de Autoriteit Persoonsgegevens sinds 1 januari torenhoge boetes uitdelen indien privacygevoelige informatie wordt gelekt. Veel organisaties beginnen zich te realiseren dat ze iets moeten doen om dergelijke data beter te beschermen. Ze weten alleen niet waar te beginnen. De KPN-case laat zien dat het integreren van security in systemen met klantinformatie makkelijker is dan veel organisaties denken.

Het zijn drukke tijden voor Dave van Stein, security consultant bij Xebia. Hij merkt dat veel bedrijven zenuwachtig worden van de vele hacks en aanvallen, en de hoge boetes die horen bij de nieuwe wetgeving. En niet zonder reden, denkt hij. "De meeste organisaties hebben best een goed incident-response-mechanisme. Als er een keertje data weglekken, kunnen ze behoorlijk adequaat reageren en het lek dichten. Daarmee kwam je tot 1 januari vaak wel weg, maar die tijd is voorbij. Aanvallen zijn niet altijd meteen duidelijk of worden direct publiekelijk bekend gemaakt. Bovendien loop je het risico een boete opgelegd te krijgen."

Veel organisaties vragen zich af: wat is het risico dat mijn systemen worden gehackt? En vooral: wat kunnen cybercriminelen met de data van mijn klanten? Veel meer dan je denkt, vertelt Van Stein. "Criminelen betalen veel geld voor een uitgebreid profiel van een persoon. Die profielen bestaan uit de combinatie van heel veel verschillende data. Het simpele gegeven dat iemand bij jou klant is kan zo'n profiel al verrijken en is dus geld waard. Dat maakt dat vandaag de dag eigenlijk ieder bedrijf potentieel interessant is voor cybercriminelen."

> "Breng securitykennis in bestaande agile teams, zodat het vanaf het eerste ontwerp wordt meegenomen"

Dat vraagt om een andere benadering van security. Een benadering die het strategische beleid van een organisatie integreert met innovatie. En dat is voor de meeste bedrijven nieuw, ziet Van Stein. "In de meeste organisaties vormen de securityspecialisten een aparte afdeling die weinig interactie heeft met andere afdelingen. Ze komen in actie als er bij een beleidswijziging een business-impactanalyse moet worden gemaakt en ze voeren periodiek risk assessments en penetratietesten uit. In de dagelijkse praktijk heeft de business weinig afstemming met deze securityspecialisten. Zeker in langere projecten maakte die scheiding het makkelijker voor alle partijen."

Iedereen loopt risico

Makkelijk was die scheiding zeker, maar verantwoord is het niet meer, vindt de security consultant. "De boetes op datalekken zijn hoog genoeg om veel bedrijven meteen de das om te doen. Daarnaast lopen veel organisaties de kans om hun 'license to operate' te verliezen. Als je als bank of hypotheekverstrekker bijvoorbeeld niet aan De Nederlandsche Bank kunt aantonen dat data van klanten bij jou veilig zijn, verlies je gewoon je banklicentie of hypotheeklicentie." Een concreet voorbeeld is DigiD. Toen Logius eiste dat er aangetoond kon worden dat het veilig was ingericht, bleek plotseling dat veel, met name kleinere, partijen zelf te weinig securitymaatregelen hadden genomen en volledig op DigiD vertrouwden. Daarmee liepen ze van de ene op de andere dag het risico hun digitale dienstverlening te moeten stoppen omdat deze niet veilig genoeg was.

SecDevOps

Alle reden dus om security hoger op de agenda te zetten. Maar dan wel op zo'n manier dat het niet te veel tijd kost of het werk veel omslachtiger maakt. Want dat is toch de angst die veel organisaties hebben. Gelukkig is die angst vandaag de dag ongegrond. Van Stein: "Door ontwikkelingen als agile werken zie je dat de business en IT veel nauwer zijn gaan samenwerken. De volgende logische stap is security hierin mee te nemen, ofwel SecDevOps. Daarmee breng je securitykennis in bestaande agile teams, zodat het vanaf het allereerste ontwerp van een nieuw systeem wordt meegenomen. Security is dan niet meer iets wat er op het laatste moment nog bovenop wordt geplakt, het maakt integraal onderdeel uit van het ontwerp van een systeem. Daardoor wordt software inherent veiliger, zonder dat het een zware belasting legt op de gebruikers."

Dit klinkt haast te mooi om waar te zijn. Traditioneel waren securityproblemen technische vraagstukken: netwerkbeveiliging, encryptie, authenticatie, autorisatie. In een wereld die wordt gedomineerd door webapplicaties, mobiele platformen, Internet of Things, big data en allerlei sociale interacties, liggen de vraagstukken op een heel ander niveau. "De eerste vraag die je je als organisatie moet stellen is: moeten we dit willen?", licht Van Stein toe. "Dat is een vraag die alleen de business kan beantwoorden. Zonder dit antwoord kan vanuit de techniek alleen maar geprobeerd worden alles zo goed mogelijk dicht te timmeren, maar de echte risico's worden daarmee niet afgevangen. Vaak moet er veel inspanning worden geleverd voor een onvolledig resultaat. Kortom, je zult security op een andere manier moeten aanvliegen en meer moeten betrekken bij de business. Neem daarbij ook de wetgeving in ogenschouw, want traditioneel vormen ook zij een aparte afdeling die niet direct betrokken is bij de business."

Multidisciplinaire teams

Multidisciplinaire samenwerking is een belangrijke eerste stap naar een oplossing. Securityspecialisten moeten de business meenemen in hun wereld en hen scholen in de basisproblematieken zodat zij veel verstandiger beslissingen kunnen nemen. Ook moeten securityspecialisten ontwikkelaars stimuleren om de securityrisico's van hun ontwikkelomgeving te leren kennen. Juridisch specialisten moeten de SecDevOps-teams wijzen op veranderingen in wet- en regelgeving, zonder meteen zelf de maatregelen te bedenken. Zij moeten fungeren als sparringpartner, niet als politieagent. Laat de agile teams vervolgens zelf nadenken over hoe zij applicaties kunnen ontwikkelen die tegemoetkomen aan die wet- en regelgeving. Van Stein: "Als je security transparant maakt, kunnen mensen van elkaar leren. Dat is noodzakelijk, want eigenlijk zou iedereen in de organisatie een bepaald basiskennisniveau moeten hebben. Die basiskennis is nu in veel organisaties niet op orde omdat niemand warmloopt voor dit onderwerp. Maak je het transparant en stel je mensen in staat om van elkaar te leren, dan maak je security ineens een stuk toegankelijker en leuker."

De KPN-case

Want ja, je kunt van security echt een onderwerp maken dat gaat leven in de organisatie. Zoals bij KPN, een van de klanten van Van Stein. "KPN had heel veel back-end systemen met eigen front-ends die ieder een klein deel van de klantinformatie ontsloten. Dat maakte het voor gebruikers – medewerkers en klanten – heel lastig om goed inzage te krijgen in de benodigde gegevens. Ook voor ontwikkeling maakte deze situatie het niet makkelijk om wijzigingen aan te brengen." Er werd besloten om een schil over die systemen heen te leggen, zodat gebruikers op één plek alle relevante informatie vonden. Die schil is agile ontwikkeld en blijft ook onderwerp van voortdurende doorontwikkeling. In eerste instantie leverde dat wrijving op met de securityorganisatie van KPN, die nog ingesteld was om op projectbasis te werken: een risk assessment aan het begin van een ontwikkeltraject, een penetratietest aan het eind, en vervolgens tussentijdse assessments wanneer er innovatie plaatsvond. Ineens kregen de securityspecialisten te maken met twintig scrumteams die iedere twee weken wijzigingen aanbrachten in de productie-omgeving.

> "Als je security transparant maakt, kunnen mensen van elkaar leren"

De security-organisatie hanteerde een lijst van een paar honderd regels. "Iedere innovatie werd op die punten gecontroleerd, een immens karwei", weet Van Stein. "Samen met KPN hebben we die lijst tegen het licht gehouden en gekeken: welke regels moeten we bij iedere sprint controleren, welke moeten we wel periodiek of op projectbasis bekijken

met SecDevOps

maar niet bij iedere sprint, en welke zijn helemaal niet relevant voor softwareontwikkeling? Op die manier is de lange lijst teruggebracht tot een tiental vragen. Afhankelijk van het antwoord op de eerste vraag verschijnt er een subset aan vervolgvragen die voor dat type ontwikkeling relevant is."

Van een paar honderd regels naar tien vragen lijkt zo op het eerste oog veel te kort door de bocht.

Maar schijn bedriegt, zegt Van Stein. "We nemen alle punten nog steeds mee, maar we kijken veel beter wanneer iets relevant is. Een deel van de eisen heeft bijvoorbeeld betrekking op de fysieke en netwerkbeveiliging van het datacenter; dat hoeft niet bij iedere sprint getoetst te worden als er ontwikkeld wordt in een eerder gevalideerd datacenter. Deze validatie laten we periodiek uitvoeren, onafhankelijk van de sprints."

Verantwoordelijkheden helder

Het grote voordeel van de korte vragenlijst is dat hoofd- en bijzaken veel duidelijker van elkaar onderscheiden worden. Alle betrokkenen bij softwareontwikkeling weten nu precies waarvoor zij verantwoordelijk zijn. Bij de lange lijst waren verantwoordelijkheden veel minder duidelijk vastgelegd, met als gevaar dat niemand zich echt eigenaar voelde. Bij de korte vragenlijst is meteen duidelijk wie hiervoor verantwoordelijk is, hoe dit raakt aan andere aspecten van security en welke dingen nu echt kritisch zijn. Het is daardoor ook makkelijker geworden om risicoprofielen toe te passen. Van Stein: "KPN weet dat ze zolang zij binnen deze spelregels blijven, ze met deze veel lagere set aan controles kunnen doorgaan. Dat geldt voor ieder ontwikkeltraject. Wil je de spelregels verruimen, dan moet je ook rekening houden met extra controles. Daardoor weet iedereen op voorhand wat de impact is van een beleidswijziging of een innovatie."

Dit heeft ertoe geleid dat KPN veel vaker en makkelijker wijzigingen kan doorvoeren, terwijl de tijd die de organisatie bezig is met het controleren van security is gedaald. Ook het aantal security-incidenten in productie is in twee jaar tijd behoorlijk afgenomen. "Door securityprocedures te vereenvoudigen en het thema vanaf het begin van ieder ontwikkeltraject mee te nemen, durft de business veel sneller met nieuwe dingen te komen", concludeert Van Stein. "Ze maken zich minder druk om wat er allemaal op hen wordt afgevuurd.

Tegelijkertijd zie je dat agile teams zich veel meer kunnen focussen op innovatie en minder tijd kwijt zijn met het fixen van dingen die zijn omgevallen. Door deze aanpak is security eigenlijk een katalysator geworden van innovatie bij KPN."