Veiliger innoveren met SecDevOps

Nieuwe tijden vragen om een nieuwe benadering

Datalekken, nieuw ontdekte kwetsbaarheden en aanvallen zijn tegenwoordig dagelijks in het nieuws. Daarnaast kan de autoriteit persoonsgegevens sinds 1 januari 2016 torenhoge boetes uitdelen indien privacygevoelige informatie gelekt wordt. Voor veel organisaties begint het ondertussen kritisch te worden om privacygevoelige informatie goed te beschermen. In de praktijk blijkt het een uitdaging om maatregelen voldoende mee te nemen tijdens innovatie. KPN en Xebia laten zien dat de integratie van securitymaatregelen tijdens ontwikkeling makkelijker is dan veel organisaties denken.

Van reactief naar proactief

De tijden veranderen. Niet alleen neemt het aantal aanvallen en hackpogingen toe, de media zit er ook bovenop en de consequenties kunnen verstrekkend zijn. Waar een kleine misser tot voor kort afgehandeld kon worden met een goede incident response, kan deze tegenwoordig direct resulteren in een forse boete. Het is dus niet langer een kwestie van reputatieschade. Een succesvolle aanval kan tegenwoordig het voortbestaan van een bedrijf in gevaar brengen.

Dat vraagt om een andere benadering van security. Een benadering vanuit het strategische beleid van een organisatie. In veel organisaties zijn de securityspecialisten ondergebracht in een eigen afdeling die weinig interactie heeft met andere onderdelen van de organisatie. Ze komen in actie als bij een beleidswijziging een business impact analyse moet worden gemaakt en ze voeren periodiek risk assessments en penetratietesten uit. In de dagelijkse praktijk vindt echter maar weinig afstemming plaats met de business- , ontwikkel- en operationele afdelingen.

Iedereen loopt risico

Veel organisaties vragen zich af hoe groot het risico is dat hun systemen worden gehackt. Onderzoek leert dat criminelen veel geld betalen voor een uitgebreid profiel van een natuurlijk persoon. Die profielen bestaan uit de combinatie van heel veel verschillende data. Zelfs een beperkte hoeveelheid data van één klant 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. Om dezelfde reden moet vrijwel ieder bedrijf kunnen aantonen dat data van klanten veilig is. Indien dat niet het geval is, dan kan de Autoriteit Persoonsgegevens overgaan tot sancties. Deze sancties worden ook publiekelijk gepubliceerd wat een bijkomend negatief effect kan hebben op de klantbeleving.

Daarnaast lopen veel organisaties de kans om hun 'license to operate' te verliezen. Als je als bank of telecom operator bijvoorbeeld niet aan De Nederlandsche Bank of Autoriteit Consument en Markt (ACM) kunt aantonen dat je processen veilig en correct werken, loop je het risico op sancties. Dit kunnen boetes zijn maar ook het intrekken van vergunningen en licenties. Een ander voorbeeld is DigiD. Toen eigenaar Logius met de 'Norm Logius ICT-Beveiligingsassessment DigiD' kwam, bleek plotseling dat veel, met name kleinere, partijen zelf te weinig securitymaatregelen hadden genomen en volledig op DigiD vertrouwden. Vaak bleek dat DigiD verkeerd geïmplementeerd was en liepen ze het risico hun digitale dienstverlening te moeten stoppen.

SecDevOps

Traditioneel waren securityproblemen technische vraagstukken: netwerkbeveili-

Dave van Stein is security consultant bij Xebia met een passie voor SecDevOps.

ging, encryptie, authenticatie, autorisatie, enzovoort. 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 of die interactie wel bijdraagt aan een business case of alleen maar aan het risico. Die vraag kan alleen beantwoord worden door de business. Zonder dit antwoord kan vanuit de techniek alleen maar geprobeerd alles zo goed mogelijk dicht te timmeren. De echte risico's worden daarmee echter niet afgevangen. Vaak moet veel inspanning worden geleverd voor een onvolledig resultaat. Kortom, security moet veel meer vanuit de business beoordeeld worden. Daarbij moet ook de wetgeving in ogenschouw worden genomen. Dit is nu nog te vaak een aparte afdeling die niet direct betrokken wordt bij het opstellen van business besluiten.

Alle reden dus om security hoger op de agenda te zetten. Voor innovatie levert dit de uitdaging dat het niet te veel tijd moet kosten of het werk veel omslachtiger maakt. Die uitdaging is tegenwoordig simpeler dan veel organisaties verwachten. Door ontwikkelingen, zoals Agile en DevOps, zie je dat de business en IT veel nauwer zijn gaan samenwerken. De logische volgende stap is dan ook de securitykennis in bestaande agile teams te integreren met SecDevOps. Zo kan de security vanaf het allereerste ontwerp van een wijziging worden mee genomen. Security is dan niet meer iets wat er op het laatst nog eens bovenop wordt geplakt, maar iets dat integraal onderdeel uitmaakt van het ontwerp van een systeem. Daardoor wordt software inherent veiliger, zonder dat het een zware belasting legt op de ontwikkelorganisatie.

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. Juridische specialisten moeten de agile teams wijzen op veranderingen in wet- en regelgeving, zonder meteen zelf allerlei maatregelen te bedenken.

De experts moeten fungeren als sparringpartner, niet als politieagent. Laat de SecDevOps teams vervolgens zelf nadenken over hoe zij applicaties kunnen ontwikkelen die tegemoetkomen aan die wet- en regelgeving. Door het transparant maken van wet- en regelgeving en de daarbij behorende security eisen kunnen mensen veel 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. Door securityproblemen bespreekbaar en transparant te maken, stel je mensen in staat om van elkaar te leren en maak je security vraagstukken ineens een stuk begrijpelijker.

De KPN-case

Eén van de Xebia-klanten die tegen deze uitdaging aanliep, is KPN. 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, zowel medewerkers als klanten, heel lastig om goed inzage te krijgen in de benodigde gegevens. Ook voor ontwikkeling maakte deze situatie het niet gemakkelijk om wijzigingen aan te brengen. Er is daarom besloten om een schil over die systemen heen te leggen, zodat gebruikers op één plek alle relevante informatie vonden. Die schil werd 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. Dit betrof een risk assessment aan het begin van een ontwikkeltraject, een penetratietest aan het eind en vervolgens tussentijdse assessments wanneer innovatie plaatsvond. Ineens kregen de securityspecialisten te maken met tientallen scrumteams die iedere twee weken wijzigingen aanbrachten in de productie-omgeving.

De KPN security policy, die voor alle systemen en processen geldt, beslaat een paar honderd regels. Iedere innovatie moet aantonen dat aan die lijst wordt voldaan. Na de overgang naar agile begon dit proces een onevenredige hoeveelheid tijd te kosten. Xebia en KPN hebben samen die lijst tegen het licht gehouden en gekeken welke regels iedere sprint relevant zijn, welke periodiek aangetoond moeten worden en welke helemaal niet relevant zijn voor softwareontwikkeling. Op die manier is de lange lijst teruggebracht tot een set van een tiental vragen. Afhankelijk van het antwoord op de eerste vraag verschijnt een subset aan vervolgvragen die voor dat type ontwikkeling relevant is.

VEEL ORGANISATIES VRAGEN ZICH AF HOE GROOT HET RISICO IS DAT HUN SYSTEMEN WORDEN GEHACKT

Van een paar honderd regels naar een tiental vragen lijkt misschien een te grote versimpeling, maar essentieel is dat die vragen dienen als filter. Er wordt beter gekeken naar 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 ontwikkeld wordt in een eerder gevalideerd datacenter. KPN controleert het datacenter nu periodiek onafhankelijk van de sprints.

Verantwoordelijkheden helder

Het grote voordeel van de korte lijst is dat hoofd- en bijzaken veel duidelijker van elkaar onderscheiden worden. Alle betrokkenen bij softwareontwikkeling weten nu precies waar zij verantwoordelijk voor zijn. Bij de lange lijst waren verantwoordelijkheden veel minder duidelijk, met het gevaar dat niemand zich echt eigenaar voelde. Hierdoor werden afwijkingen vaak veel te laat geïdentificeerd. Bij de korte vragenlijst is meteen duidelijk: "Wie is hiervoor verantwoordelijk", "Hoe raakt dit andere aspecten van security" en "Welke aspecten zijn nu echt kritisch".

Het is daardoor ook gemakkelijker geworden om risicoprofielen toe te passen. Ieder team binnen KPN weet nu wat de spelregels zijn. Zolang je binnen deze spelregels blijft, kun je met deze veel kortere set aan controles doorgaan. Wil je de spelregels verruimen, dan moet je ook rekening houden met aanvullende controles. Daardoor weet iedereen op voorhand wat de impact is van een beleidswijziging of een innovatie.

Dit heeft ertoe geleid dat security kennis nu breder belegd is, KPN veel vaker en makkelijker wijzigingen kan doorvoeren en de tijd die innovatie kwijt is om te kijken of aan het juiste securitylevel voldaan is, verminderd is. Ook is het aantal security-incidenten is in twee jaar tijd behoorlijk gedaald.

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. 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. Eigenlijk is security een katalysator geworden van innovatie bij KPN. ■

MULTIDISCIPLINAIRE SAMENWERKING IS EEN BELANGRIJKE EERSTE STAP NAAR EEN OPLOSSING