Auteurs: Dave van Stein is security transformation consultant bij Xebia Security. Hij helpt organisaties met het oplossen van uitdagingen op het gebied van security, compliance en privacy in Agile en DevOps ontwikkelomgevingen. Dave is te bereiken op dvanstein@xebia.com. Edzo Botjes is antifrAgile architect bij Xebia Security. Hij houdt zich met name bezig met de invloed van menselijk gedrag in complexe systemen. Edzo is bereikbaar op ebotjes@xebia.com.

Goed nieuws voor de CISO

Krijg je organisatie mee door de business te begrijpen en te sturen op waarde

Als CISO ben je verantwoordelijk voor de beveiliging van business en IT-processen. Een duidelijke rol. Toch blijkt dat in de praktijk, door de kloof tussen security en IT-development, die rol niet zo helder is. Wanneer is deze kloof ontstaan en hoe kunnen we zorgen dat developers de waarde van security inzien?

"Je carrière is over!", hoorde Steve Katz zijn vrouw roepen. Het was 1995 en Citigroup, waar Steve net een maand werkte, kwam in het nieuws als slachtoffer van een Russische hack. Vrij snel daarna werd Steve Katz de eerste CISO ooit met een hele duidelijke opdracht: "Je weet dat we zijn gehackt en we geven je een blanco check. We willen zeker weten dat dit niet nog een keer gebeurt. We willen dat je de beste information securityafdeling ter wereld opzet" (1). Met Steves carrière is het helemaal goed gekomen; hij werd een held en legde de basis voor hoe we nu nog steeds tegen informatiebeveiliging aankijken.

Zes jaar later verzuchtte Alistair Cockburn: "Ik had nooit verwacht dat deze groep agilisten het ooit over iets substantieels eens zou worden." Een groep van 17 developers had zich net drie dagen opgesloten in een berghut om een praktische oplossing te vinden voor hun stelling: 'om succesvol te kunnen zijn in de nieuwe economie en snel het internettijdperk in te kunnen bewegen, moeten bedrijven zich ontdoen van hun bureaucratische karikaturen en ondoorzichtige processen' (2). Hoewel hun opvattingen over softwareontwikkeling enorm verschilden, was het de groep gelukt om vier basisprincipes te definiëren in het Agile Manifesto. Hiermee was de Agile-revolutie in gang gezet wat de drijvende kracht werd achter DevOps en cloud.

Hoewel, of misschien wel doordat, deze gebeurtenissen los van elkaar hebben plaatsgevonden, is hier de kloof tussen Information Security en IT-development ontstaan. Eerst werd security losgeweekt van IT-development en omgevormd tot een autonoom orgaan met eigen verantwoordelijkheden. Vervolgens is IT-development gaan versnellen met continue verandering en verbetering als mantra. Deze kloof moeten we nu zien te overbruggen. Maar hoe doe je dat? Hoe combineer je 35 jaar aan zorgvuldig opgebouwde security-zekerheden met de geplande onzekerheid van agile?

Toegevoegde waarde

Agile en DevOps dwingen een organisatie continu na te denken over toegevoegde waarde. Als ergens de toegevoegde waarde niet duidelijk van is, wordt de stekker eruit getrokken. Security is geen uitzondering en als security officer moet je leren hierop in te spelen en over na te denken. Dit blijkt in de praktijk een uitdaging voor veel risk en security professionals. Simpelweg wijzen op externe verplichtingen of een intern beleid is niet langer voldoende; je moet kunnen aangeven waarom wat je doet en vraagt noodzakelijk is.

Helaas hebben we de luxe niet om het op zijn beloop te laten. Als het over security of privacy gaat, kan het agile principe van fail fast, fail often snel desastreuze gevolgen hebben. Vandaag de dag sta je met een datalek meteen vol in de schijnwerpers. Een incident kan direct grote financiële gevolgen hebben of een zorgvuldig opgebouwde reputatie tenietdoen. Hoe zorg je ervoor dat agile developers security niet als bureaucratisch bestempelen, maar serieus nemen omdat ze de waarde ervan inzien? Simpel, zorg dat je een 'security sales pitch' hebt die de volgende elementen bevat: rust, marketing, snelheid.

Security geeft rust

Het eerste onderdeel van je pitch is 'security is een verzekering.' Security-incidenten leiden vaak tot ongepland werk zoals code herschrijven, delen van het systeem opnieuw ontwerpen of de infrastructuur wijzigen. Omdat ontwikkelteams in een agile omgeving volledig verantwoordelijk zijn voor productkwaliteit – en in DevOps ook voor Incident Response – komt dit werk voor hun rekening. Kunnen (en willen) deze teams het risico nemen dat zij hun planning om moeten gooien of hun nachtrust op moeten offeren voor het corrigeren van een security-incident? Hoewel agile verandering omarmt, geldt dat niet voor ongepland werk. Dat willen agile teams juist minimaliseren. Gebruik om je verhaal extra kracht bij te zetten een actueel verhaal, of nog beter, een gefundeerde risico-kosten analyse. Denk hierbij terug aan de kracht van de 'holy shit-factor' zoals beschreven werd in het interview met Eelco Dykstra in iB-magazine nr. 5 van 2020 (3). Linksom of rechtsom, zorg dat je je pitch op orde hebt!

Security als marketing

De hersteltijd van een incident is natuurlijk niet de enige manier om waarde uit te drukken. De gevolgschade van een security-incident kan wel eens veel meer impact hebben. Wat doe je als klanten het vertrouwen in je product verliezen en weglopen als gevolg van een incident? Het inkomen van de organisatie kan zomaar als sneeuw voor de zon verdwijnen. Klanttevredenheid is een van de belangrijkste meetpunten voor een agile team. Om succesvol te zijn in een competitieve markt is het van belang aantoonbaar beter te zijn dan de concurrent. Door vele datalekken en hacks beginnen klanten gevoeliger te worden voor de manier waarop bedrijven met security en privacy omgaan. De impact van imagoschade is daarom een argument waar agile teams gevoelig voor zouden moeten zijn. Een transparante security-aanpak is positieve reclame.

Gitlab is een sterk voorbeeld van een cultuur van radicale transparantie. Alle processen en maatregelen zijn volledig inzichtelijk en ook alle incidenten worden publiekelijk bekendgemaakt (4). Gitlab ontving veel positieve reacties op hoe zij omgingen met een incident waarbij een productiedatabase werd gewist en veel klanten hun data kwijt waren. Gitlab meldde dit meteen publiekelijk en was heel transparant over alle vervolgacties. Dit maakte duidelijk dat dit iedereen had kunnen overkomen en dat Gitlab in dergelijke situaties serieus en professioneel te werk gaat. Openheid over hoe je omgaat met security wordt steeds belangrijker als marketing. Als security officer kan je hier handig gebruik van maken - door security onderdeel te maken van de marketingstrategie, lift je mee op dit budget.

Security als snelheidskatalysator

Om ontwikkelteams volledig over de streep te trekken moeten we nog een stap verder gaan en ons richten op activiteiten die (directe, aantoonbare) waarde opleveren. Dit lijkt onmogelijk, maar de sleutel tot succes hebben we al lang in onze zak: de risicogebaseerde aanpak. Helaas is dit begrip inmiddels behoorlijk uitgehold en houdt het in de praktijk niet meer in dan statische workflows met verplichte processtappen. Het is noodzakelijk om deze aanpak grondig om te gooien.

In de loop der tijd zijn securityvraagstukken flink veranderd. Waar er voorheen vaak sprake was van puur technische vraagstukken, hebben incidenten tegenwoordig vaak gelijk een impact op bedrijfsvoering of klanten. Helaas werken veel security experts nog in een bubbel, zonder dagelijkse interactie met business en IT. Zoals ik al eerder aangaf in dit artikel, is dit de kloof die we moeten dichten. De realiteit is non-stop aan het veranderen en daar kunnen we alleen mee omgaan door echt samen te werken met de teams die daadwerkelijk risico's kunnen voorkomen. Deze samenwerking moet in ieder geval de volgende drie cruciale onderdelen bevatten:

1. **Risicoanalyses**
   Om te bepalen welke maatregelen noodzakelijk zijn moeten risicoanalyses vaak en snel worden gedaan. Een jaarlijkse business impact assessment of pentest is simpelweg niet meer voldoende. Technieken als threat modeling (5), wheels of misfortune (6) en TRIZ-analyses (7) stellen ontwikkelteams in staat om deze analyses vaak en snel zelf uit te voeren en, indien nodig, een expert in te schakelen. Hierdoor wordt het simpel om mogelijke dreigingen snel in kaart te brengen en een afweging te maken of verdere actie nodig is.
2. **Securitycultuur**
   Security experts zijn over het algemeen goed in het voorspellen van dreigingen en het zien van gaten in de spelregels. Zij zijn dus bij uitstek de aangewezen personen om teams hierin te ondersteunen. Om niet volledig afhankelijk te zijn van specialisten, is het zaak een cultuur te introduceren waarbij teams op een positieve manier worden betrokken bij security. Maak security weer leuk en toegankelijk zodat iedereen zich medeverantwoordelijk gaat voelen. Op deze manier kan de benodigde schaalgrootte bereikt worden.
3. **Automatiseer processen**
   Door de meest simpele maatregelen te automatiseren, hebben teams daar geen omkijken naar en kunnen zij zich focussen op de business. De normale technische flow door het ontwikkelproces zou ook automatisch de veilige manier moeten zijn. Vergelijk het met het ombouwen van wegen met verbodsborden, slagbomen en snelheidsbegrenzers naar een situatie met adviezen, vangrails en airbags. De beschikbare capaciteit wordt maximaal benut en ernstige ongelukken worden voorkomen. Dit vergt helaas vaak wel een flinke investering, maar zodra teams security omarmen, gaan ze er zelf mee aan de slag!

Security verkopen is cruciaal

Agile en security worden vaak gezien als twee dingen die lastig samengaan. Het is echter een kwestie van hoe je het verpakt. Agile teams willen tevreden klanten. Als agile security officer is het zaak om duidelijk te maken dat security niet een moetje is, maar juist iets waar alle stakeholders veel voordeel uit kunnen halen! (8)

Referenties

(1) https://cybersecurityventures.com/backstory-of-the-worlds-first-chief-information-security-officer/
(2) http://Agilemanifesto.org/history.html
(3) https://www.pvib.nl/actueel/ib-magazines/ib-magazine-2020-5/downloaden
(4) https://docs.gitlab.com/ee/security/README.html
(5) https://www.threatmodelingmanifesto.org/
(6) https://cloud.google.com/blog/products/management-tools/shrinking-the-time-to-mitigate-production-incidents
(7) https://www.triz.co.uk/what-is-triz
(8) https://articles.xebia.com/being-an-Agile-security-officer