License to Operate

Auteur: CISO Kadaster
Vastgesteld: Security Board

15 januari 2024

Versie 1.0

Inhoudsopgave

Inleiding

Onze dienstverlening aan de maatschappij stoelt op onze informatiehuishouding: onze registers, applicaties en IT-landschap. Die informatiehuishouding is een balans van functionaliteiten in eigen applicaties en systeemsoftware van derden (Java, Oracle, Google, Microsoft, etc.).
Omdat cyberdreigingen toenemen en cybercriminelen elk systeem, netwerk of organisatie als doelwit zien is cybersecurity als randvoorwaarde of ‘License to Operate’ vanzelfsprekend geworden.

Om onze dienstverlening weerbaar en robuust te maken en houden hanteert het Kadaster deze License to Operate. Deze licentie stelt voorwaarden waaraan onze informatiehuishouding moet voldoen om te mogen functioneren. Het niet voldoen aan deze voorwaarden zal stapsgewijs consequenties hebben en kunnen resulteren in afsluiting van de betreffende dienst.

Daar waar in dit document gesproken wordt over het Kadaster en 'wij’ kan het ook de contractuele aansturing betreffen van leveranciers voor onze datacenters of andere IT-diensten.

Updates

Regelmatig brengen 'derden’ (Java, Oracle, Google, Microsoft, etc.) updates uit voor hun software. Deze updates zijn gericht op nieuwe functionaliteiten, het wegnemen van bugs en het verbeteren van de beveiliging. Dat verbeteren van de beveiliging is noodzakelijk doordat telkens nieuwe kwetsbaarheden in software worden gevonden. Hackers buiten die kwetsbaarheden bijna gelijk uit om toegang te verkrijgen tot organisatie, informatie te stelen, ransomware uit te rollen, etc.

Iedere update die wij niet kunnen installeren verhoogt ons risico op een gijzeling, datalek, of misbruik van onze informatiehuishouding.

Systeemsoftware

Wij zorgen dat we de laatste versies van systeemsoftware gebruiken. Dus deze is up-to-date: dat wil zeggen de laatste versie is geïnstalleerd binnen één week na uitkomen van de update en bij high geclassificeerde patches binnen 24 uur

Indien systeemsoftware niet geüpdatet kan worden, omdat daardoor de werking van een applicatie wordt verstoord, krijgt de betreffende applicatie een door security en BOI gezamenlijk te bepalen overgangsperiode voor het realiseren van deze aanpassing. Na de betreffende periode wordt de update alsnog uitgevoerd. Onze leveranciers volgen onze richtlijn en zorgen dat zij up-to-date systeemsoftware gebruiken en leveren.

Secure Software Development

Wat voor die 'derden’ geldt, geldt ook voor ons. Onze eigen applicaties bevatten ongewild kwetsbaarheden. Ontwikkelen van software is mensenwerk, en daarin sluipen soms foutjes die de functionaliteit kunnen verstoren alsook een haakje kunnen zijn voor misbruik. Vanwege haar vrij unieke bedrijfsprocessen, wordt er bij het Kadaster veel maatwerksoftware gebouwd. De manier waarop deze ontworpen en geprogrammeerd wordt, en ook de daarbij gebruikte opensource "standaard bouwblokken" bepalen voor een groot deel de veiligheid van onze informatie.

Daarom is het essentieel dat de ontwikkelrichtlijnen voor veilige software worden gebruikt, zoals TIOBE of ISO 25010. Met behulp van geautomatiseerde tooling onderzoeken we onze software op dergelijke fouten. De kwaliteit en robuustheid van onze applicaties, en daarmee onze dienstverlening neemt daardoor toe.

Software en systeem hardening

Om risico's verder te reduceren zetten wij overbodige functies uit. Ons configuratiemanagement richt zich erop onze softwarecomponenten zo veilig mogelijk te kunnen gebruiken door altijd bewust te kiezen om alleen die functionaliteit aan te zetten die ook echt noodzakelijk is, veilige waarden toe te kennen aan beveiligingsinstellingen en standaard accounts en wachtwoorden te wijzigen.

Pentesten en kwetsbaarheidsscans

Ondanks al onze inspanningen kan het zijn dat wij iets over het hoofd zien in onze ontwikkelingen en de uitrol van updates. Om onze applicaties en omgeving nog robuuster te maken onderwerpen we deze aan pentesten en kwetsbaarheidsscans. Voor pentesten vragen we externe specialisten onze omgeving en applicaties voorafgaande aan in-productie-name, alsook in productie, te onderzoeken op kwetsbaarheden. Daarnaast voeren we zelf geautomatiseerde kwetsbaarheidsscans uit. Als wij iets over het hoofd hebben gezien komt dat aan het licht en kunnen we dit verbeteren.

Software Bill of Materials

Bij het gebruik van software en libraries van derden moeten we ons bewust zijn van kwetsbaarheden in onderliggende componenten. Daarom maken wij een zorgvuldige afweging óf en hoe wij deze inzetten. Wij rationaliseren deze keuze en zorgen dat we geen software en libraries gebruiken uit risicolanden.

Documentatie

Documentatie, de kers op de pudding. Doordat wij goed documenteren hoe onze applicaties en systemen werken, waar ze hun informatie vandaan halen, hoe de geautomatiseerde koppelingen verlopen, wie de verantwoordelijken zijn, in welke processen de applicatie gebruikt wordt, welke afnemers er zijn van de informatie en alle andere relevante informatie over de werking en samenhang van applicaties, infrastructuur en systeemsoftware zijn wij onder andere in staat changes zorgvuldig uit te voeren, in crisissituaties snel te handelen, incidenten op te lossen.

Deze documentatie leggen wij vast (met een verwijzing daarnaar) in de CMDB.

Platformonafhankelijke software ontwikkeling

In het kader van onze software ontwikkeling streven we naar platformonafhankelijkheid. Dit betekent dat we ons in de (systeem)software die we gebruiken beperken tot functies die als algemene internet- en Cloud standaard worden beschouwd. We mijden bewust het gebruik van specifieke, geavanceerde functies die weliswaar kortetermijnoplossingen bieden, maar uiteindelijk onze flexibiliteit kunnen beperken, update-processen kunnen verstoren en ons vermogen om soepel over te stappen naar andere platforms of systemen kunnen verminderen.

Critical and High patches

Vanuit onze omgeving krijgen wij van 'derden’ patches aangeleverd. Deze patches zijn geclassificeerd op urgentie ten aanzien van risico's rondom de beveiliging. De beoordeling van critical en high wordt intern bijgesteld op basis van de impact voor het Kadaster. Wij richten onze processen zodanig in dat critical en high geclassificeerde patches met voorrang uitgevoerd kunnen worden. Dankzij onze documentatie in de CMDB weten we welke applicaties geraakt kunnen worden door de patch zodat deze tijdig aangepast kunnen worden.

High geclassificeerde patches worden binnen één week doorgevoerd, de critical patches binnen 24 uur. Dit betekent dat we met onze collega's afspraken hebben gemaakt over mogelijk overwerk en prioritering in dergelijke situaties.

Internet facing

Voor diensten die direct aan het internet zijn verbonden zorgen we dat partners, afnemers en burgers kunnen zien dat wij deze beschermd hebben en dat zij veilig hun gegevens kunnen invullen en/of aanbieden. Dit stellen we veilig door het gebruik van certificaten, uitgegeven door externe partijen, die de encryptie en authenticiteit van onze diensten waarborgen. Intern ondersteunen we deze certificaten met maatregelen zoals firewalls en constante monitoring door ons Security Operations Center (SOC). Voor interne netwerkverbindingen tussen applicaties, versleutelen we data in transit wanneer deze als 'vertrouwelijk' of 'geheim' is geclassificeerd

Internetstandaarden

Door gebruik te maken van moderne internetstandaarden zorgen we ervoor dat onze websites betrouwbaar zijn. We hanteren de lijst met verplichte standaarden van Forum Standaardisatie op basis van ‘Pas toe of leg uit’.
Op regelmatige basis toetsen wij onze websites op het gebruik van deze standaarden. Dat doen wij door gebruik te maken van de testtool Internet.nl, een initiatief van het Platform Internetstandaarden.

GITC

Het Kadaster werkt met General IT Controls om grip te houden op de werking en het onderhoud van de IT, inclusief security controls.

Waarschuwingen

Wij zorgen dat wij van externe bronnen -zoals NCSC- informatie betrekken rondom waarschuwingen van kwetsbaarheden in en/of misbruik van (systeem)software en/of websites. De informatie wordt geoperationaliseerd naar mitigerende acties die in de organisatie worden uitgevoerd.

Applicaties

Applicaties zijn:

- Ingericht volgens de architectuur-richtlijnen, beveiligingsrichtlijnen, ontwikkelstandaarden en voorbrengingsprocessen en maken gebruik van de standaard door het Kadaster geleverde (cloud)platformen;
- Getoetst met behulp van tooling op hardening en programmeerfouten;
- Aantoonbaar Cloud Ready gebouwd;
- Geschikt om te draaien op de meest recente versie van systeemsoftware of kunnen daartoe binnen 24 uur of één week voor aangepast worden afhankelijk van classificatie van patches;
- Gedegen gedocumenteerd (met verwijzing vastgelegd) in de CMDB, in ieder geval voor wat betreft een BIA, CSA, herstelplan, procesbeschrijvingen, architectuurdocumentatie en configuratie items (hardware en software items). De CSA fungeert als evaluatie-instrument om te beoordelen of een applicatie voldoet aan de License to Operate;
- Waar nodig voorzien van certificaten;
- Onderworpen aan pentesten op basis van risico-inschatting omvang wijzigingen, en resultaten van pentesten zijn binnen één maand verholpen of geaccepteerd als risico;
- Gekoppeld met de security monitoring diensten.

Consequenties dienstverlening

Iedere omgeving waarbij (nog) niet voldaan wordt aan de License to Operate wordt:

- Niet gekoppeld aan het internet
- Afgescheiden van de rest van het netwerk
- Voorzien van extra monitoring vanuit het SOC

Indien een bestaande applicatie niet voldoet aan de License to Operate, wordt een overgangsperiode vastgesteld waarbinnen deze applicatie aan deze vereisten gaat voldoen. In deze periode zal alle inspanning gericht zijn op de non-functionele aspecten van de applicatie om zo snel mogelijk te kunnen voldoen aan de License to Operate. Daardoor kunnen er in deze periode geen vernieuwingswerkzaamheden plaatsvinden.
Na afloop van de overgangsperiode wordt de situatie beoordeeld door een security expert en kan worden gekozen de periode te verlengen of de licentie definitief in te trekken. Een nieuwe applicatie die niet voldoet, wordt niet in productie genomen.

Het intrekken van de licentie of het niet in productie nemen wordt als eerste gemeld bij de directeur en betreffende management van ODR en tevens worden de CISO en de directeuren BOI en DGV hierover geïnformeerd. Deze kunnen met in acht name van een overgangsperiode besluiten de applicatie tijdelijk stil te leggen totdat de problemen zijn verholpen.

Personele en Organisatorische consequenties

Het toepassen van de License to Operate heeft personele en organisatorische consequenties:

- Prioritering binnen de lijn voor oplossen van dreigingen
- Teams moeten beschikbaar zijn om versneld aanpassingen door te voeren
- Dienstverlening kan beperkt worden doordat niet voldaan wordt aan de voorwaarden
- Piketregelingen voor aan te wijzen functies t.b.v. aanpassingen (is ook nodig i.v.m. crisisorganisatie)

Voordelen

- De kans dat een incident escaleert naar crisis of calamiteit wordt kleiner (nooit 0)
- Bij een crisis en/of calamiteit kan sneller gehandeld worden
- Het aantal verstoringen zal kleiner zijn en sneller opgelost kunnen worden
- Dienstverlening aan de maatschappij zal een hogere mate van zekerheid bieden
- Potentiële schade voor personen/privacy wordt beperkter