DATTO ZET VOL IN OP BSIMM-BEVEILIGINGSMODEL

Maak security inzichtelijk

Hoe meet je veiligheid? Deze vraag houdt securityspecialisten volop bezig, want implementeren van cybersecurity is één, maar vaststellen hoe veilig de eindklant dan is, is vers twee. Aan de hand van een security framework kun je de beveiliging langs een meetlat leggen. Datto koos voor BSIMM, een framework dat de successen en fouten van verschillende organisaties naast elkaar legt. *Tekst: Ryan Weeks*

Datto, leverancier van onder meer business continuity & disaster recovery, hecht logischerwijs veel waarde aan de veiligheid van de eigen infrastructuur en applicaties. Daarnaast wijst het bedrijf al langere tijd op de verantwoordelijkheid van het kanaal, waaronder de MSP's die partner zijn van Datto, om de eindklant te adviseren op het gebied van cybersecurity. Een van de meest essentiële zaken is het omarmen van een gedegen cybersecurity framework als basis.

BSIMM staat voor 'Building Security In Maturity Model'. Het legt initiatieven op het gebied van cybersecurity naast elkaar en kwantificeert daarnaast de applicatiebeveiliging van verschillende organisaties. Daaronder vallen bedrijven en instellingen van over de hele wereld, in alle takken van industrie en handel. Het doel is om erachter te komen wat elke organisatie uniek maakt en zo te leren hoe het bij andere bedrijven beter kan. Een framework is kortom een set standaarden, aanbevelingen en best practices voor cybersecurity. BSIMM is niet het enige security framework. Het meest bekend is vermoedelijk het NIST Cybersecurity Framework van het Amerikaanse standaardeninstituut. Een andere bekende is OWASP Open SAMM. Ook het welbekende ISO heeft zijn ISO 27001/27002 securitystandaard.

BSIMM als startpunt

Datto koos voor BSIMM als standaard framework. Dat kwam op een organische manier tot stand. Vanaf 2019 ging het bedrijf op zoek naar de beste manieren om zijn Application Security programma te verbeteren. Het startpunt was BSIMM, maar voornamelijk bedoeld als inspiratie. Tegelijk deed Datto evaluaties van andere security frameworks, zoals NIST. Hoewel het de bedoeling is dat hiervan zeker onderdelen in Datto's Application Security Framework worden opgenomen, zijn deze als geheel niet ideaal. Voornaamste kritiekpunt is dat ze zelfbevestigend zijn en weinig ruimte bieden voor onpartijdige assessment van derden. Bovendien zijn ze, aldus Datto, relatief statisch, en dat kan niet in een wereld waar beveiliging in hoog tempo onderhevig is aan veranderingen. De keuze viel daarom op het uitbouwen van de betrokkenheid bij BSIMM, omdat de koers en inhoud ervan bepaald worden door inmiddels meer dan 120 aangesloten bedrijven, waaronder Cisco en PayPal. Het framework krijgt regelmatig updates en blijft daardoor relevant.

De keuze om actief deel te nemen aan een cybersecurity framework volgt uit de verantwoordelijkheid die Datto naar eigen zeggen heeft voor het beschermen van zichzelf en de aangesloten MSP-partners. Dat dit geen loze woorden zijn, blijkt uit het feit dat al in 2018 erop werd geanticipeerd dat er aanvallen zouden kunnen komen op de 'MSP supply chain'. Dat zijn aanvallen op leveranciers van MSP-oplossingen – zoals Datto – of op MSP's zelf, met als resultaat dat de eindklanten worden geraakt. Dit werd bewaarheid in juli 2021, toen een grootschalige aanval op een leverancier van remote managementoplossing werd gebruikt om ransomware onder de eindklanten te verspreiden. Het toeval wilde dat tegelijkertijd het succesvolle BSIMM-assessment plaatsvond van Datto's eigen en pas gelanceerde Remote Monitoring & Management oplossing.

Ryan Weeks is Chief Technology Officer bij Datto

BSIMM is, zoals gezegd, (onder meer) een kwantitatieve beoordeling. Een van de resultaten van het assessment was dat Datto beschikt over een niveau van volwassenheid van de beveiliging in dit nieuwe onderdeel van 5,7 jaar. Dat wil zeggen: hoewel het nieuwe software was, was de beveiliging op een niveau van dat van bedrijven die softwarebeveiligingsprogramma's hebben die al 5,7 jaar draaien. In december 2021 volgde een assessment van Datto Networking, met vergelijkbare resultaten. Voor dit jaar staan meerdere assessments gepland, waarbij als eerste Datto's Business Continuity Suite aan de beurt is.

> **De koers en inhoud van BSIMM worden bepaald door inmiddels meer dan 120 aangesloten bedrijven**

Bug bounty

Parallel aan dit alles vond in maart van dit jaar de lancering plaats van het Datto Vulnerability Disclosure Program v 2.0. Dit programma stimuleert partners, gebruikers en ethische hackers om kwetsbaarheden en veiligheidslekken in Datto software, hardware en diensten te melden, met een beloning als het om een echte kwetsbaarheid gaat, de melder de eerste is en het door Datto opgelost is. Versie 1.0 van het programma startte in november 2020 en leverde veel respons op. Er werden diverse serieuze bedreigingen gevonden die uiteindelijk allemaal werden opgelost.

Interne expertise

Dat dit nu genoemd wordt in één adem met het BSIMM-framework is geen toeval. Het installeren van een programma voor het melden van kwetsbaarheden, ook wel een 'bug bounty program', is sinds kort een van de vereisten voor deelname aan BSIMM. Datto koos er daarbij bewust voor om dit niet uit te besteden aan een derde partij, zoals vaak gebeurt.

Datto ontdekte dat bedrijven die dit uitbesteden zelf vaak niet beschikken over de juiste interne expertise en capaciteiten. Maar als beveiligingsbedrijf beschikt Datto wel over die expertise. Bovendien wil Datto zoveel mogelijk betrokken zijn bij zijn MSP-partners, waarbij het bedrijf niet te ver af wil komen te staan van de dagelijkse praktijk en zelf de teugels zoveel mogelijk in handen wil houden. ■