Global Headquarters

Genetec Inc.
2280 Alfred Nobel Blvd.
Montreal, Quebec H4S 2A4
Canada

T: +1 514.332.4000

Press release

EU Cyber Resilience Act verhoogt eisen van fysieke beveiligingstechnologie

Genetec introduceert richtlijnen die beveiligingsprofessionals helpen vragen te stellen aan hun leverancier over productbeveiliging, transparantie en support

Amsterdam, 14 september 2026 —Genetec Inc. ("Genetec"), wereldwijd marktleider op het gebied van software voor fysieke beveiliging, heeft vandaag richtlijnen gepubliceerd waarmee fysieke security professionals kunnen beoordelen hoe hun technologieaanbieders connected producten ontwerpen, onderhouden en ondersteunen. Dit wordt steeds belangrijker nu de EU Cyber Resilience Act (CRA) strengere eisen stelt aan cybersecurity gedurende de volledige levenscyclus van producten.

De CRA stelt cybersecurity-eisen aan producten met digitale onderdelen die in de Europese Unie worden verkocht. De wetgeving benadrukt veilige productontwikkeling, management van kwetsbaarheden, transparantie op het gebied van cybersecurity en voortdurende productondersteuning gedurende de volledige levenscyclus van een product.
Hoewel de wetgeving in eerste instantie vooral van toepassing is op fabrikanten, heeft de CRA ook gevolgen voor organisaties die verbonden devices distribueren, installeren, inkopen en gebruiken.

"In de Cyber Resilience Act staat veel beschreven op het gebied van 'secure by design' en lifecyclemanagement; principes waar Genetec zich al jaren voor inzet", aldus Mathieu Chevalier, Principal Security Architect bij Genetec Inc. "Doordat de CRA de verwachtingen rond productbeveiliging en transparantie verhoogt, biedt het fysieke security professionals een duidelijk kader om technologieaanbieders en de cyberweerbaarheid van hun producten op de lange termijn te beoordelen."

De meldingsverplichtingen voor kwetsbaarheden op grond van de CRA zijn vanaf 11 september jl. van kracht. Hierdoor zullen organisaties in toenemende mate afhankelijk zijn van hun technologieaanbieders om aan de nieuwe eisen op het gebied van cybersecurity en het omgaan met kwetsbaarheden te voldoen. Om te helpen beoordelen in hoeverre leveranciers

hierop zijn voorbereid, adviseert Genetec organisaties om 5 belangrijke vragen te stellen aan potentiële technologieaanbieders:

Vraag 1: Hoe lang zijn er security updates en support beschikbaar?

De CRA benadrukt het belang van het waarborgen van productbeveiliging gedurende de volledige levenscyclus van producten. Het is daarom belangrijk dat security professionals inzicht hebben in hoelang de leverancier updates zal leveren, hoe er met kwetsbaarheden omgegaan wordt en welke ondersteuning ze krijgen wanneer producten aan het einde van de lifecycle zijn. De CRA-regelgeving verplicht fabrikanten om gedurende minimaal vijf jaar beveiligingsupdates te leveren en kwetsbaarheden te managen. Langdurige ondersteuning is daarmee een belangrijke factor.

Vraag 2: Is cybersecurity ingebouwd vanaf het begin van het productontwerp?

De principes van Secured by Design en Secure by Default staan centraal in de CRA. Daarom is het belangrijk te vragen toe te lichten hoe cybersecurity wordt geïntegreerd in het ontwerp, de ontwikkeling en het testen van producten, gedurende de volledige levenscyclus van het product.

Vraag 3: Hoe identificeert, meldt en verhelpt de leverancier kwetsbaarheden?

Er is geen software die vrij is van kwetsbaarheden. De manier waarop een leverancier hiermee omgaat, zegt veel over zijn inzet voor wat betreft cybersecurity. Let op een goed ingericht programma voor het management van kwetsbaarheden, met onder meer regelmatige beveiligingstests, een beleid voor gecoördineerde openbaarmaking van kwetsbaarheden, risicogebaseerde oplossingen zonder onnodige vertraging, het veilig aanbieden van beveiligingsupdates en duidelijke informatie over verholpen kwetsbaarheden.

Vraag 4: Is de provider transparant over de manier waarop deze zelf met cybersecurity omgaat?

Cybersecurity is een gedeelde verantwoordelijkheid. Verantwoordelijke leveranciers zijn transparant over de manier waarop zij hun producten ontwikkelen, testen en onderhouden, en bieden klanten en integrators duidelijke richtlijnen voor veilige implementatie.

Vraag hoe de leverancier de beveiliging van zijn producten regelmatig test en evalueert, hoe hij communiceert over kwetsbaarheden en beveiligingsupdates en welke richtlijnen hij biedt voor het verder versterken en beveiligen van systemen.

Vraag 5: Hoe ondersteunt de leverancier cyberweerbaarheid op de lange termijn?

De cybersecurity van een product stopt niet na de implementatie. Samenwerken met betrouwbare technologiepartners is daarom essentieel. Organisaties moeten goed onderzoeken hoe de leverancier de supporttijd van een product bepaalt en communiceert, hoe hij omgaat met kwetsbaarheden, beveiligingsupdates levert, veilige operations ondersteunt en het einde van de levensduur van het product beheert.

Daarnaast is het belangrijk om te vragen welk bewijs de leverancier kan leveren om aan te tonen dat het product gedurende de volledige levenscyclus voldoet aan de geldende cybersecurityvereisten.

“Organisaties die het best zijn voorbereid op het omgaan met toekomstige cyberdreigingen, zien cybersecurity als een doorlopend partnerschap en niet als een eenmalige inkoopbeslissing”, concludeert Chevalier. “De CRA helpt deze aanpak te versterken door gemeenschappelijke verwachtingen te stellen op het gebied van transparantie, zorgvuldig management van kwetsbaarheden en langdurige productondersteuning. Dit komt ten goede aan fabrikanten, integrators en de organisaties die afhankelijk zijn van verbonden fysieke beveiligingssystemen.”

Meer informatie over best practices voor fysieke security systemen is hier te lezen: https://www.genetec.com/trust-cybersecurity

--einde persbericht--