Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2122

Vragen van het lid **Kathmann** (GroenLinks-PvdA) aan de Minister van Justitie en Veiligheid over *het bericht «Geheime afmeldcodes van duizenden alarmsystemen opvraagbaar door softwarefout»* (ingezonden 24 april 2024).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 28 juni 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2023–2024, nr. 1742.

Vraag 1
Bent u bekend met het bericht «Geheime afmeldcodes van duizenden alarmsystemen opvraagbaar door softwarefout»?[1]

Antwoord 1
Ja.

Vraag 2
Is het u bekend welke (Rijks-)overheidsorganisaties en vitale organisaties getroffen zijn door het lek in de systemen van SMC en Securitas? Zo ja, kunt u een overzicht aanleveren? Zo nee, waarom niet?

Antwoord 2
Nee, dat is mij niet bekend. SMC en Securitas zijn zelf verantwoordelijk voor het informeren van hun klanten over het lek. Vanwege de aard en beperkte impact van het lek heeft het Nationaal Cyber Security Centrum (NCSC) geen reden gezien om hierover verdere navraag te doen bij Rijksoverheidsorganisaties en vitale aanbieders.

Vraag 3
Zijn alle (Rijks-)overheidsorganisaties en vitale organisaties die getroffen zijn door het lek in de systemen van SMC en Securitas inmiddels op de hoogte van het lek? Is het u bekend of zij allemaal inmiddels maatregelen hebben getroffen?

[1] BNR, 11 april 2024, Geheime afmeldcodes van duizenden alarmsystemen opvraagbaar door softwarefout (https://www.bnr.nl/nieuws/tech-innovatie/10544662/geheime-afmeldcodes-van-duizenden-alarmsystemen-opvraagbaar-door-softwarefout).

ah-tk-20232024-2122
ISSN 0921 - 7398
's-Gravenhage 2024

Antwoord 3
Zowel SMC als Securitas heeft te kennen gegeven dat na eigen onderzoek geen indicatie van actief misbruik van het lek is waargenomen bij bedrijven en andere organisaties die gebruik maken van de systemen van SMC en Securitas. Daarnaast hebben zij aangegeven aanvullende maatregelen te hebben genomen zoals het offline halen van kwetsbare systemen, het resetten en verwijderen van de oude afmeldcodes en het inrichten van een nieuw verificatieproces. (Rijks-)overheidsorganisaties en vitale organisaties zijn daarmee voldoende beschermd.
Het NCSC heeft besloten geen algemeen advies op te stellen vanwege de maatregelen die door SMC en Securitas zijn getroffen, de aard van de kwetsbaarheid en de daardoor geringe impact op haar doelgroep.

Vraag 4
Heeft u contact gehad met SMC en Securitas over dit incident? Zo ja, welke stappen gaat u de komende periode zetten om dit probleem af te wikkelen? Zo nee, waarom niet?

Antwoord 4
Het NCSC en het Digital Trust Center (DTC) hebben meerdere malen contact gehad met SMC en Securitas over de kwetsbaarheid. Met name gelet op de toelichting van de zijde van SMC en Securitas in die gesprekken over de aard en beperkte impact van dit lek op bedrijven en andere organisaties is door het NCSC besloten hierover geen verdere actie te ondernemen ten behoeve van de eigen doelgroep. Zie ook antwoord op vraag 3.

Vraag 5
Gaat u getroffen bedrijven helpen om de risico's van dit lek zo goed en snel mogelijk te mitigeren? Welke middelen zijn hiervoor beschikbaar? Zo nee, waarom niet?

Antwoord 5
Zie antwoord op vraag 3 en vraag 4.
Het product waarin de kwetsbaarheid is gevonden, was een zogenaamd end-of-life product. Dit betekent dat dit product niet meer werd onderhouden of ondersteund door de leverancier. Het gebruik van dit soort producten brengt een risico met zich mee. Het Nationaal Cyber Security Centrum (NCSC) heeft diverse adviesproducten op de website over risicomanagement in het algemeen en het omgaan met producten waarvan het onderhoud en ondersteuning door de leverancier afloopt in het bijzonder. In de toekomst moeten nieuwe digitale producten die op de Europese markt worden gebracht voldoen aan cybersecurityeisen conform de Cyber Resilience Act. Dit betreft onder meer het verplicht en gratis leveren van veiligheidsupdates, zolang je mag verwachten dat een product kan worden gebruikt.

Vraag 6
Hebben gevoelige gegevens en locaties gevaar gelopen door dit lek? Zo nee, waar blijkt dat uit?

Antwoord 6
SMC en Securitas hebben aangegeven dat er na onderzoek geen indicatie van misbruik is waargenomen. Het Nationaal Cyber Security Centrum (NCSC) heeft zelf ook geen indicaties hiervoor waargenomen.
Van de zijde van SMC en Securitas is aangegeven dat het initieel leek alsof met de kwetsbaarheid onrechtmatig toegang verkregen kon worden tot fysieke locaties. Echter, na onderzoek van deze twee partijen bleek de kwetsbaarheid alleen zogenaamde telefonische afmeldcodes te betreffen richting de centrale. Om een alarm daadwerkelijk uit te schakelen moet lokaal een code fysiek worden ingevoerd. Deze code is alleen bekend bij de klant en was ook niet onderdeel van de kwetsbaarheid. Zonder het invoeren van deze lokale code kan het alarm niet worden uitgeschakeld.

Vraag 7
Kunt u aangeven of dit lek meer alarmcentrales heeft getroffen dan enkel Securitas en SMC?

Antwoord 7
Van andere alarmcentrales is niet bekend of deze zijn getroffen.

Vraag 8
Kunt u aangeven of de aantallen, van minstens 26.000 getroffen organsaties en personen, kloppen? Hoeveel organisaties en personen zijn er volgens u getroffen?

Antwoord 8
Het Nationaal Cyber Security Centrum (NCSC) kan dit aantal niet bevestigen, met name ook omdat het zelf geen meldingen hierover van organisaties heeft ontvangen. Zie beantwoording vraag 6.

Vraag 9
Kunt u aangeven of het Nationaal Cyber Security Centrum (NCSC) of een andere overheidsorganisatie betrokken is bij het onderzoek dat SMC zelf uitvoert naar de scope van het lek? Worden de uitkomsten daarvan gedeeld met de Minister en andere relevante partijen, zoals de Autoriteit Persoonsgegevens?

Antwoord 9
Het SMC is primair verantwoordelijk voor het onderzoek naar de scope van het lek en het delen van de uitkomsten daarvan. Het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center (DTC) hebben meerdere malen contact gehad met SMC en Securitas over de kwetsbaarheid. Zoals aangegeven in het antwoord op vraag 6 is het onderzoek inmiddels afgerond en zijn de uitkomsten gedeeld met het Ministerie van Justitie en Veiligheid. Op grond van de AVG is elke organisatie die te maken heeft met een datalek zelf verantwoordelijk om daar melding van te doen bij de Autoriteit Persoonsgegevens. SMC en Securitas hebben aangegeven melding van het onderhavige lek te hebben gedaan bij de Autoriteit Persoonsgegevens.

Vraag 10
Kunt u aangeven of de softwareontwikkelaar die het lek heeft aangetroffen zich had kunnen melden bij het NCSC om een Coordinated Vulnerability Disclosure te doen?

Antwoord 10
Deze persoon heeft een Coordinated Vulnerability Disclosure, ook wel CVD-melding genoemd, bij het NCSC gedaan.

Vraag 11
Wat kunt u doen om het doen van Coordinated Vulnerability Disclosures bij NCSC breder bekend te maken bij mensen die werkzaam zijn in de IT-sector?

Antwoord 11
Op de website van het Nationaal Cyber Security Centrum (NCSC) is veel informatie te vinden over Coordinated Vulnerability Disclosures (CVD). Dit betreft onder meer informatie over hoe personen een CVD-melding kunnen doen om technische kwetsbaarheden te melden bij het Nationaal Cyber Security Centrum(NCSC). Binnen de community van onderzoekers en ethische hackers is het CVD-beleid van het Nationaal Cyber Security Centrum (NCSC) over het algemeen goed bekend.

Vraag 12
Kunt u deze vragen afzonderlijk beantwoorden?

Antwoord 12
Ja.