Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

31 288 Hoger Onderwijs-, Onderzoek- en Wetenschapsbeleid

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1176

BRIEF VAN DE MINISTER VAN ONDERWIJS, CULTUUR EN WETENSCHAP

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 21 januari 2025

Met deze brief informeer ik uw Kamer over de gebeurtenissen ten aanzien van de cyberaanval bij de Technische Universiteit Eindhoven (TU/e) op zaterdag 11 januari jongstleden. Daarbij is een hack geconstateerd op de systemen van de TU/e, wat aanleiding is geweest voor de universiteit om preventief en tijdelijk alle systemen buiten werking te stellen. Dit had consequenties voor het onderwijs en onderzoek van de universiteit. Colleges gingen niet door en tentamens werden uitgesteld. Dat heeft impact gehad op docenten, onderzoekers en studenten. De TU/e heeft in goed overleg met o.a. de medezeggenschap er alles aan gedaan om de gevolgen zo beperkt mogelijk te houden. Inmiddels zijn het onderwijs en onderzoek aan de universiteit volledig hervat.

Ik heb besloten uw Kamer te informeren via deze brief omdat de instelling te maken heeft gehad met een grote verstoring van het onderwijs en daarmee het onderwijs niet toegankelijk was voor studenten. Dit doe ik indachtig het gestelde in de motie Martens-America[1].

Allereerst wil ik graag mijn waardering uitspreken voor iedereen bij de TU/e en de andere betrokken organisaties die dag en nacht hebben gewerkt om de problemen als gevolg van de cyberaanval zo snel als mogelijk te adresseren en onderwijs en onderzoek weer mogelijk te maken. Door snel en adequaat handelen zijn de gevolgen voor de studenten, onderzoekers en andere medewerkers van de TU/e beperkt gebleven.

Gebeurtenissen TU Eindhoven

Zaterdagavond 11 januari 2025 is door de TU/e verdachte activiteit waargenomen op het netwerk van de universiteit. Diezelfde avond is,

[1] Kamerstuk 36 560 VIII, nr. 13, Motie van het lid Martens-America over actief aan de Kamer rapporteren wanneer een onderwijsinstelling niet vrij, veilig of toegankelijk is voor studenten.

kst-31288-1176
ISSN 0921 - 7371
's-Gravenhage 2025

gezien de op dat moment ingeschatte omvang en impact van de cyberaanval, door de TU/e besloten om alle systemen preventief offline te halen. Zondag 12 januari 2025 is mijn ministerie op de hoogte gesteld van de situatie en zijn studenten, onderzoekers en andere medewerkers geïnformeerd dat het onderwijs en onderzoek op maandag 13 januari niet door kon gaan. Door de TU/e is een onderzoek gestart naar de getroffen infrastructuur en toedracht met als doel om zo snel en veilig mogelijk alle systemen weer te activeren. De politie is bij dit onderzoek betrokken. Het technische en forensische onderzoek naar de precieze oorzaak van de hack en naar mogelijke verdachten loopt nog. Hierover kunnen door de TU/e nog geen mededelingen worden gedaan.

Relevante informatie is met belanghebbenden, zoals de andere onderwijsinstellingen, gedeeld zodat ook zij waar nodig maatregelen konden nemen. De bestaande bestuurlijke en expertnetwerken tussen instellingen en sectoren op het gebied van cyberveiligheid zijn in de loop van de week benut voor informatie-uitwisseling, kennisdeling en preventie. Experts in alle instellingen werkten op basis van protocollen en afspraken samen om ook de infrastructuur in andere onderwijsinstellingen veilig te houden. SURF heeft hierbij als CSIRT voor het onderwijs[2] een centrale rol gespeeld. Vanwege haar toezichtstaak op het waarborgen van de continuïteit van het onderwijs van instellingen in het hoger onderwijs staat ook de Inspectie van het Onderwijs in contact met de TU/e en laat de inspectie zich door de TU/e informeren over het lopend onderzoek.

Uiteindelijk is na afstemming binnen de universiteit met diverse (onderwijs)directeuren, examencommissies en de medezeggenschap, besloten het onderwijs voor de hele week niet door te laten gaan en de onderwijskalender tot aan de zomer met één week op te schuiven om op deze manier de gevolgen voor studenten zo beperkt mogelijk te houden. De TU/e heeft inmiddels gecontroleerd en stap voor stap de systemen herstart waarbij de prioriteit is gegeven aan de systemen die nodig waren voor onderwijs en tentaminering. Er zijn door de TU/e geen constateringen van dataversleuteling of gestolen data gedaan en de TU/e heeft te allen tijde controle gehouden over haar infra en systemen.

Overige gebeurtenissen

Op woensdag 15, donderdag 16 januari en vrijdag 17 januari hebben diverse onderwijsinstellingen in het zuiden van het land, en later ook daarbuiten, te maken gehad met verstoring van de ICT-voorzieningen als gevolg van een grote DDoS-aanval tegen instellingen, waardoor het SURF-netwerk vol liep. Naar de DDoS-aanvallen en eventueel verband met de cyberaanval op de TU/e wordt door SURF, zoveel mogelijk samen met het Nationaal Cyber Security Centrum (NCSC)[3], nog onderzoek gedaan. Er is aangifte gedaan bij de politie. Naar aanleiding van de aanvallen zijn door SURF mitigerende maatregelen getroffen, zowel curatief als preventief. De aanvallen zijn steeds na enkele uren gestopt. Ook met betrekking tot dit voorval is binnen en tussen de sectoren informatie en kennis gedeeld conform de bestaande sectorale afspraken rond cyberweerbaarheid, en is verhoogde paraatheid ingesteld.

---

[2] SURFcert is het Computer Emergency Response Team voor onderwijs en onderzoek. SURFcert biedt hulp bij het opzetten van een Computer Security Incident Response team (CSIRT) en ondersteuning en advies bij cyberaanvallen.

[3] Het NCSC is onderdeel van het Ministerie van Justitie en Veiligheid en is de Rijksorganisatie die zich bezig houdt met digitale veiligheid. Het NCSC identificeert en duidt risico's en trends, verbind verschillende partijen op het gebied van digitale veiligheid en kan ondersteuning en advies geven.

Vervolg

De TU/e heeft aangekondigd dat er een externe evaluatie zal plaatsvinden naar de crisisaanpak van de instelling en heeft toegezegd deze evaluatie, voor zover mogelijk, openbaar te delen zodat ook anderen van deze aanpak kunnen leren. Dit is heel waardevol, zowel binnen de sector onderwijs als daarbuiten. Het past in de aanpak en verdere ambities van het verhogen van cyberweerbaarheid door hbo, wo en mbo instellingen waarin instellingen nauw samenwerken, kennis delen en van elkaar leren om als sectoren cyberveilig te zijn en blijven.

De cyberdreiging neemt toe, zoals ook het Cyber Security Beeld Nederland 2024 laat zien.[4] Dit geldt voor de gehele samenleving, waaronder ook het hoger onderwijs. Daarbij bestaat er geen 100% veiligheid. Ondanks de professionele wijze waarop TU/e haar cyberweerbaarheid heeft ingericht, laat het incident bij de TU/e dit ook weer zien. Dit maakt dat het van belang is dat instellingen ook in de toekomst goed voorbereid blijven op de risico's die dit met zich meebrengt voor hun instelling en voor de sectoren gezamenlijk. Het zo veel mogelijk voorkomen van aanvallen is daarbij van groot belang (preventie), maar weerbaarheid betekent ook correcte respons om de continuïteit te waarborgen als een aanval niet voorkomen kan worden (curatief). De instellingen in het vervolgonderwijs zijn zich hiervan goed bewust, hebben er ervaring mee opgedaan en handelen hiernaar. Er wordt gewerkt met bestuurlijke afspraken met OCW ter versterking van de cyberweerbaarheid van het mbo, hbo en wo met als kernelementen dat elke mbo-, hbo- en wo-instelling aan een vooraf afgesproken normenkader voldoet, aangesloten is op een mechanisme om 24/7 dreigingen te monitoren (aansluiting Security Operations Center) en dat elke instelling zich periodiek ook extern laat auditen. Deze afspraken worden regulier gemonitord en waar nodig bijgesteld en verbeterd in samenspraak met de sectoren en SURF[5]. Het is aan de instelling om – vanuit oogpunt van hun zorg voor de kwaliteit en continuïteit van onderwijs en onderzoek en in lijn met de bestuurlijke afspraken over verhoging van cyberweerbaarheid – voorbereid te zijn op incidenten en adequate afhandeling daarvan. SURF vervult hierin onder andere met SURFcert[6] een belangrijke rol.

Kamerlid Six Dijkstra vroeg tijdens het Vragenuur van 14 januari 2025 aan Staatssecretaris Struyken of er zicht is op de stand van de cyberweerbaarheid in het hoger onderwijs. Ik ben voornemens uw Kamer nog dit kwartaal per brief te informeren over deze stand van zaken en welke maatregelen er genomen worden om het niveau van cyberweerbaarheid in het gehele vervolgonderwijs verder te verhogen. In deze brief zal ik, na overleg met de Minister van Justitie en Veiligheid, ook ingaan op het al dan niet aanwijzen van hbo- en wo-instellingen als essentiële of belangrijke entiteit als bedoeld in de aankomende Cyberbeveiligingswet en daarmee onder de toepasselijkheid van deze wet brengen. Hierover ben ik in gesprek met alle betrokken partijen om mij te beraden op de impact hiervan.

De Minister van Onderwijs, Cultuur en Wetenschap,
E.E.W. Bruins

---

[4] Bijlage bij Kamerstuk 26 643, nr. 1229
[5] Kamerstuk 31 288, nr. 922
[6] SURFcert is het Computer Emergency Response Team voor onderwijs en onderzoek. Bij cyberaanvallen biedt SURFcert ondersteuning en advies.