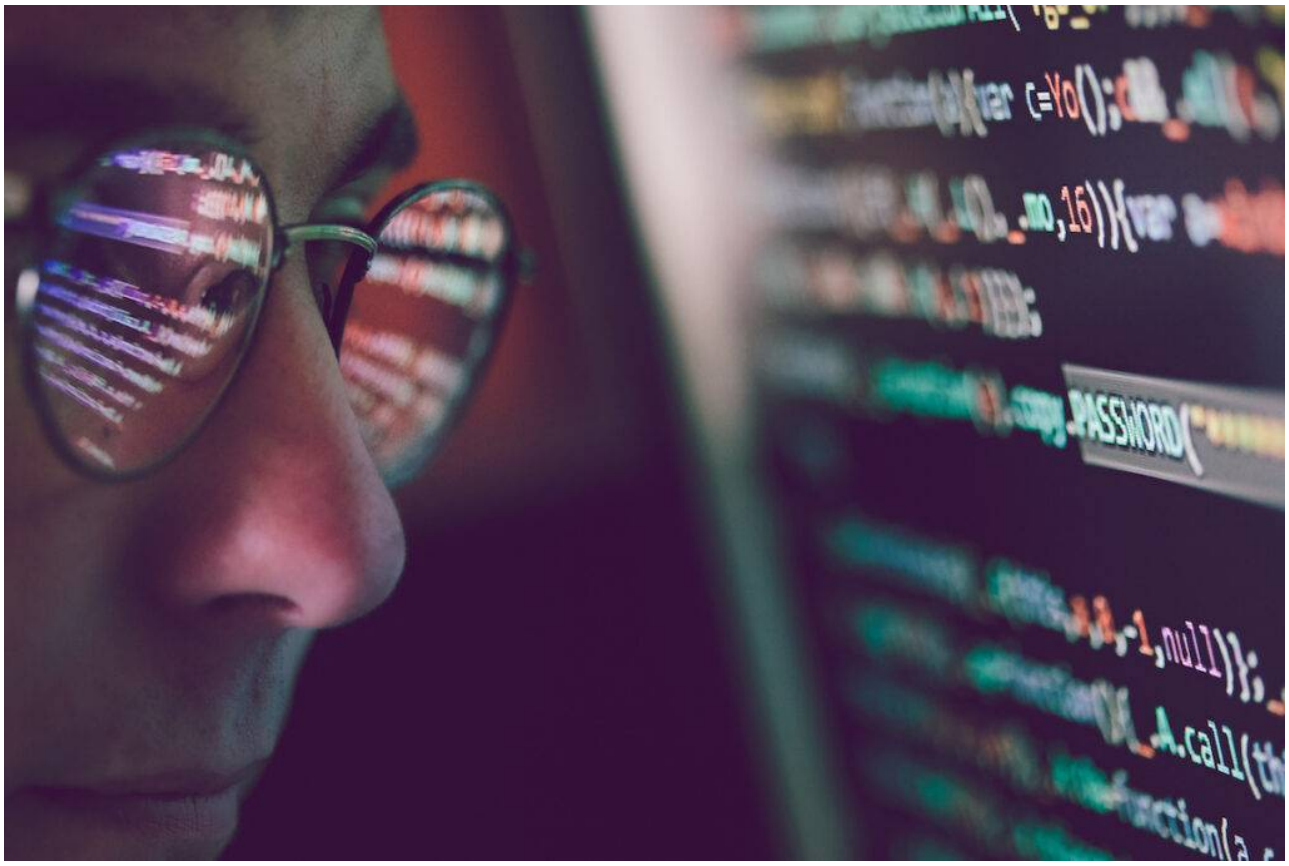
NWO, NRO en SIA na ransomware hack weer opgestart

22 maart 2021



NWO kondigde tien dagen geleden aan dat, als alles volgens planning verliep, de werkzaamheden in de week van 22 maart weer opgestart zouden worden. Vorige week werd duidelijk dat het subsidieproces vandaag, 22 maart, opgestart zou worden. Het opstarten van de werkzaamheden betekent in de praktijk dat de NWO nu eerst voorrang zal geven aan lopende subsidierondes waar aanvragers op een resultaat wachten. Werkzaamheden die niet direct met rondes of lopende projecten te maken, worden iets langzamer opgestart.

Opstartproces van enkele weken

De komende dagen en weken gaat NWO ervoor zorgen dat de aangepaste teksten op de call-pagina's zo snel mogelijk gepubliceerd worden. Dat is met name van belang voor calls waarvan de deadline in de komende weken aflopen. Dit kan voor deze calls betekenen dat indieners na indienen geïnformeerd zullen worden over het aangepaste tijdpad.

Hoewel NWO er in geslaagd is het merendeel van de informatie te herstellen, kan het nog steeds gebeuren dat sommige zaken missen. Zo is een deel van de informatie uit de week voorafgaand aan 13 februari verloren gegaan. Dat geldt overigens niet voor de informatie uit ISAAC. Die is compleet hersteld.

Alle berichtend die tussen 6 februari en 7 maart naar NWO gestuurd zijn, zijn niet aangekomen. NWO en haar medewerkers doen hun uiterste best om iedereen twee van dienst

te zijn, maar de organisatie vraagt begrip voor het feit dat dit de komende periode in sommige gevallen meer tijd zal vragen dan u normaal gewend bent.

Ransomware hack NWO

De hack van de netwerkservers van NWO werd medio februari ontdekt. Sindsdien was het voor NWO, Regieorgaan SIA en Regieorgaan NRO onmogelijk het primaire proces – de financiering voor de wetenschap – uit te voeren. Daarom werden alle activiteiten die daarmee samenhangen, van het openen van nieuw calls tot het beoordelingsproces, tot nader order stilgelegd. Mails aan medewerkers van NWO, SIA, NRO, TKI HTSM en LNVH kwamen niet aan, en bleven onbeantwoord. Zoals nu bekend is, waren die berichten ook niet meer te herstellen.

Z-Cert, de instantie die de sector Zorg & welzijn ondersteunt op het gebied van (cyber)security, meldde onlangs nog in zijn eerste Cyberdreigingsbeeld dat er een duidelijke groei is van het aantal cyberaanvallen. Het gaat daarbij zowel om aanvallen met malware zoals phishing en vooral ransomware als om aanvallen die gericht zijn op het onderbreken van de dienstverlening (DDOS).