Cybersecurity-oefening ISIDOOR

Gezamenlijk oefenen belangrijk voor digitale veiligheid

Afgelopen juni deden zo'n 96 organisaties uit de publieke en private sector mee aan de grootste nationale cybercrisisoefening tot nu toe, ISIDOOR 2021. Bijna 1.500 deelnemers uit vitale sectoren zoals drinkwatervoorziening, nucleair, energie, infrastructuur en het bankwezen hebben geoefend – samen met verschillende overheden, zoals ministeries, veiligheidsregio's, politie en het OM. *Waarom is zo'n grootschalige oefening nodig en wat hebben de drinkwaterbedrijven ervan geleerd?*

De driedaagse oefening ISIDOOR 2021 werd georganiseerd door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC) en had tot doel om de informatie-uitwisseling, samenwerking en coördinatie bij een cybercrisis te oefenen. Tijdens de oefening werden afspraken, structuren en processen uit het Nationaal Crisisplan Digitaal geoefend aan de hand van een crisisscenario.

Verschillende cyberincidenten

Voor ISIDOOR werden verschillende soorten cyberincidenten gesimuleerd: een aanval door een ander land door middel van phishing mails, ransomware-aanvallen of het binnendringen in systemen via een kwetsbaarheid in een softwareprogramma. Hierdoor kon er tijdens de simulatie bijvoorbeeld fictief gevoelige bedrijfsinformatie worden buitgemaakt en konden vitale processen worden verstoord. Voorbeelden daarvan zijn klantenservices en websites die slecht bereikbaar waren en/of foutieve informatie bevatten, of vertragingen in het betalingsverkeer. Door te oefenen kan tijdens een echte digitale crisis sneller en adequater gehandeld worden.

Hester Somsen, plaatsvervangend NCTV en directeur Cybersecurity.

'Een cyberaanval kan directe gevolgen hebben in het leven van mensen. Kijk naar de files die ontstonden door de problemen met Citrix omdat thuiswerken niet meer mogelijk was. Maar we moeten ook voorbereid zijn op ernstigere situaties met meer maatschappelijke ontwrichting. Allereerst moet de cyberveiligheid bij alle organisaties op orde zijn. En als het dan toch misgaat, moet je daar met elkaar klaar voor zijn. Daarom is oefenen zo belangrijk. Dat draagt bij aan informatie-uitwisseling tussen partijen, versterkt de samenwerking en laat de noodzaak tot coördinatie zien. Driekwart van de organisaties is opgeschaald tot bestuurlijk niveau. Dat betekent ook dat we cyberveiligheid op de tafel van bestuurders hebben gekregen. Gezien het belang hoort het onderwerp daar thuis', aldus Hester Somsen, plaatsvervangend NCTV en directeur Cybersecurity.

Weerbaarheid van Nederland verhogen

Het aantal cyberincidenten neemt nog ieder jaar toe en ons land moet blijvend werk maken van het verhogen van de weerbaarheid tegen dit soort aanvallen. Daarom zet het kabinet ook in op een nationaal oefen- en testprogramma, waarvan ISIDOOR 2021 onderdeel is. Het afgelopen jaar zijn meerdere voorbeelden te noemen, zoals de kwetsbaarheid in SolarWinds Orion en in Microsoft Exchange, waardoor veel bedrijven kwetsbaar waren.

Hans de Vries, directeur NCSC: 'De digitale weerbaarheid van Nederland verhogen, bewustzijn creëren en voorbereiden op digitale aanvallen is dus erg belangrijk. Hierin is gezamenlijk oefenen een belangrijk onderdeel. Daardoor leren deelnemers dezelfde taal te spreken, krijgen ze inzicht in elkaars belangen en problemen én kunnen ze elkaar in het echt sneller en beter vinden. Omdat een cyberincident zich per definitie snel ontwikkelt en veel impact heeft, is oefenen nodig om maatschappelijke ontwrichting en grote (financiële) schade te voorkomen.'

Hans de Vries, directeur NCSC.

Lessons learned

De lessen uit deze oefening worden meegenomen in de voorbereiding van betrokken organisaties op cyberincidenten en verwerkt in de plannen en procedures, waaronder het Nationaal Crisisplan Digitaal. Aan de hand daarvan kunnen organisaties zich verder ontwikkelen en werken aan hun flexibiliteit, weerbaarheid en veerkracht. En dat is nodig. Want één ding is zeker: de cybercrisis van morgen is anders dan de cybercrisis die gisteren is geoefend.

ISIDOOR 2021

De oefening bestond dit keer uit een operationeel/tactisch deel en een bestuurlijk deel. Het eerste deel van de oefening focuste zich op operationeel/tactisch samenwerken tussen het cyberdomein en andere organisaties, maar ook met partijen betrokken vanuit crisisbeheersing, zoals diverse Departementale Coördinatiecentra Crisisbeheersing (DCCs) en een aantal veiligheidsregio's.

Ook werd de nationale crisisstructuur geactiveerd, waardoor het bestuurlijke deel van ISIDOOR geoefend kon worden in de vorm van een Interdepartementale Commissie Crisisbeheersing (ICCb). Hierin waren meerdere departementen vertegenwoordigd.

De evaluatie van ISIDOOR kan als input meegenomen worden in de actualisering van het Nationaal Crisisplan Digitaal. Ook kunnen de geleerde lessen van ISIDOOR als best practice dienen voor de organisatie van cyberoefeningen in de toekomst.