COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

Datum: 23 augustus 2021
Betreft: Wijziging Wet beveiliging netwerk- en informatiesystemen i.v.m. uitbreiding bevoegdheid MinJenV

Zijne excellentie,

U heeft een wijziging op de Wet beveiliging netwerk- en informatiesystemen (Wbni) voorgelegd voor een internetconsultatie. Stichting Z-CERT gaat hier graag op in.

Digitale weerbaarheid verhogen

Nederland digitaliseert, iedere sector heeft hierdoor te maken met een groeiend IT-oppervlak. Tevens is het aantal kwetsbaarheden onverminderd hoog en neemt de digitale dreiging toe. Het is voor organisaties vaak een uitdaging om grip te krijgen, en te houden, op informatiebeveiliging. Computer Emergency Response Teams (CERT's) spelen een vitale rol in de informatievoorziening t.a.v. organisaties, of het nu gaat om dreigingen, kwetsbaarheden, of om hulp bij incidenten. Het effect van CERT's is onmiskenbaar positief.

Helaas moet ook vastgesteld worden dat niet alle organisaties vallen onder een CERT, of OKTT. Dit plaatst deze organisaties in een onvoordelige positie t.o.v. organisaties die wel onder een CERT vallen. Bijvoorbeeld, wanneer een ernstige kwetsbaarheid bekend wordt gemaakt zullen organisaties (in de regel) worden geïnformeerd door de overkoepelende partijen. Z-CERT bijvoorbeeld zal in dergelijke gevallen zorginstellingen bellen of e-mailen ten einde organisaties kenbaar te maken dat zij kwetsbaar zijn.

Echter, de lijst van kwetsbare partijen is soms groot, en Z-CERT kan alleen zorgorganisaties informeren. Voorts is dit een taak die volgens Z-CERT beter gepositioneerd zou zijn bij het Nationaal Cyber Security Centrum (NCSC). Door het NCSC de mogelijkheid te geven organisaties te informeren die buiten het reikveld van de CERT's en OKTT's vallen zal het aantal cybersecurity incidenten af nemen. Tevens wanneer een deel van deze taak bij de organisaties 'objectief kenbaar tot taak' (OKTT) zou kunnen worden gelegd, zou dit naar Z-CERT haar mening een positief effect sorteren.

Bovenstaande is slechts één voorbeeld van een situatie waarbij deze wijziging bij zou dragen aan de verhoging van de digitale weerbaarheid van heel Nederland. Denk bijvoorbeeld ook aan situaties waarbij dreigingsinformatie of kenmerken van incidenten gedeeld kunnen worden. Z-CERT heeft in haar eigen doelgroep al vele malen mee mogen maken dat het (tijdig) delen van kwetsbaarheden, dreigings- of incidentinformatie incidenten heeft voorkomen.

Z-CERT is daarom voorstander van deze wijziging van de Wbni.

Met vriendelijke groet,

Steven van Baardewijk
Stichting Z-CERT

Stichting Z-CERT
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
KvK 67374972