Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Risicobeheersing

Hoe het NCSC u daarbij kan helpen

Toegestane verspreiding: TLP WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP: WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp). Ontvangers mogen de informatie uit deze handreiking delen binnen en buiten hun organisatie, daarnaast mag de informatie openbaar publiek gemaakt worden.

Uw reacties zijn welkom op info@ncsc.nl

Risicobeheersing

Het Nationaal Cyber Security Centrum kan uw organisatie helpen met het op orde brengen van de beheersing van digitale risico's. Dat kan door te adviseren over de inrichting van risicomanagement en door het bieden van ondersteuning bij het inventariseren van de digitale risico's en dreigingen. Deze informatie-brochure legt uit wat deze diensten betekenen.

Bij een effectieve en efficiënte cybersecurityaanpak treft uw organisatie maatregelen die zijn afgestemd op de digitale risico's[1]. Om passende maatregelen te kunnen treffen, is het van belang dat de digitale dreigingen en de daarbij horende risico's op een goede manier in kaart zijn gebracht en beoordeeld. Dit proces heet risicoanalyse.

De digitale wereld is continue in beweging. Ook nieuwe risico's vragen om uw aandacht. Van bekende risico's is het verstandig om periodiek vast te stellen of deze nog actueel zijn. Ook van geïmplementeerde mitigerende maatregelen doet u er goed aan om deze periodiek te beoordelen op effectiviteit. Om deze redenen is het belangrijk om een risicoanalyse met enige regelmaat te herhalen. Het proces waarmee een organisatie blijvend zicht en grip houdt op risico's heet risicomanagement.

Voor wie is deze informatiebrochure?

Het NCSC is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. De Rijksoverheid en organisaties in vitale sectoren zijn de belangrijkste afnemers van de expertise van het NCSC. Het NCSC ondersteunt hen bij het treffen van maatregelen om de continuïteit van hun dienst te waarborgen en bij incidenten te herstellen. Wanneer uw organisatie onderdeel is van de rijksoverheid of een vitale aanbieder is, dan kunt u een beroep doen op het NCSC voor ondersteuning bij risicoanalyses of voor advies over risicomanagement.

Advies over risicomanagement

Bij cybersecurity komt vaak een hoop techniek kijken. Deze techniek kan bestuurders en managers zonder IT-achtergrond afschrikken. Echter, goede cybersecurity bestaat niet alleen maar uit techniek. Het bevat ook een belangrijk organisatorisch deel. Op tactisch niveau is dat het dragen van de verantwoordelijkheid over hetgeen we met cybersecurity willen beveiligen, inclusief de bijbehorende digitale risico's. Op strategisch niveau is dat organiseren dat deze verantwoordelijkheden op een goede manier belegd zijn binnen de organisatie. Een niet goed

[1] Zie hoofdstuk 7 in het CSBN: https://www.ncsc.nl/documenten/publicaties/2021/juni/28/csbn-2021

ingerichte organisatorische kant van cybersecurity vergroot de kans op een niet goed ingerichte technische kant van cybersecurity.

Het NCSC kan u adviseren over de inrichting van risicomanagement[2]. Dat kan door middel van een presentatie of door eenvoudig in gesprek te gaan met de betrokken medewerkers binnen uw organisatie.

Ondersteuning bij een risicoanalyse

Een belangrijk onderdeel van risicobeheersing is het inzichtelijk maken van de voor uw relevante risico's. Hoewel het uitvoeren van een risicoanalyse geen hogere wiskunde hoeft te zijn, kan het voor sommigen toch lastig zijn om daar op een goede manier een eerste stap mee te maken. Het NCSC kan u daarmee op weg helpen.

In het geval van een serieuze dreiging staat het NCSC natuurlijk altijd voor u klaar, maar in de overige gevallen is ons doel dat u zelfstandig een risicoanalyse leert uit te voeren. Het NCSC faciliteert dan de eerste risicoanalyse voor u. De tweede analyse begeleidt u zelf, waarbij het NCSC aanwezig is ter ondersteuning. De derde analyse doet u zelfstandig en het NCSC is achteraf beschikbaar om de analyse en de resultaten met u door te spreken. Daarna is het aan u om volledig zelfstandig risicoanalyses binnen uw organisatie uit te voeren.

Risicoanalyses zijn er in meerdere vormen, want niet iedere situatie is hetzelfde. U heeft bijvoorbeeld te maken met een dreiging vanuit een geavanceerde actor. U wil zicht hebben op de voor u relevante digitale dreigingen. U wil de door de BIO gestelde risicoafweging kunnen maken of u wil een gedegen technische blik werpen op uw ICT-infrastructuur. Op basis daarvan wilt u passende maatregelen kunnen treffen. Het NCSC kan u helpen bij deze uitdagingen. Het kan ook zijn dat u beschikt over een eigen aanpak, maar graag de kennis en ervaring van het NCSC bij uw risicoanalyse wil hebben of een kritische reactie op die aanpak wil hebben. Ook dan staat het NCSC u graag bij.

Meer weten?

Wilt u meer weten over de manier waarop het NCSC u kan adviseren over de inrichting van risicomanagement of kan ondersteunen bij de uitvoering van een risicoanalyse? Heeft u een daadwerkelijk hulpverzoek en wilt u daarvoor een afspraak inplannen? Bel ons dan op 070-751 5555 of stuur een e-mail naar info@ncsc.nl.

[2] Zie ook onze factsheet: https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

November 2021