Veilig Digitaal Ondernemen

Op naar een cyberweerbaar bedrijfsleven

Platform voor Informatie Beveiliging (PvIB)

12-11-2019

digital trust center.

Wat ga ik vertellen?

1. **Wat is het Digital Trust Center (DTC)?**
2. **Waarom stimuleren we samenwerken?**
3. **Hoe kunnen wij jullie helpen?**
4. **Hoe hebben anderen dit aangepakt?**
5. **Hoe willen jullie het aan gaan pakken?**

digital trust center.

Wie ben ik?

Rajko Smaak

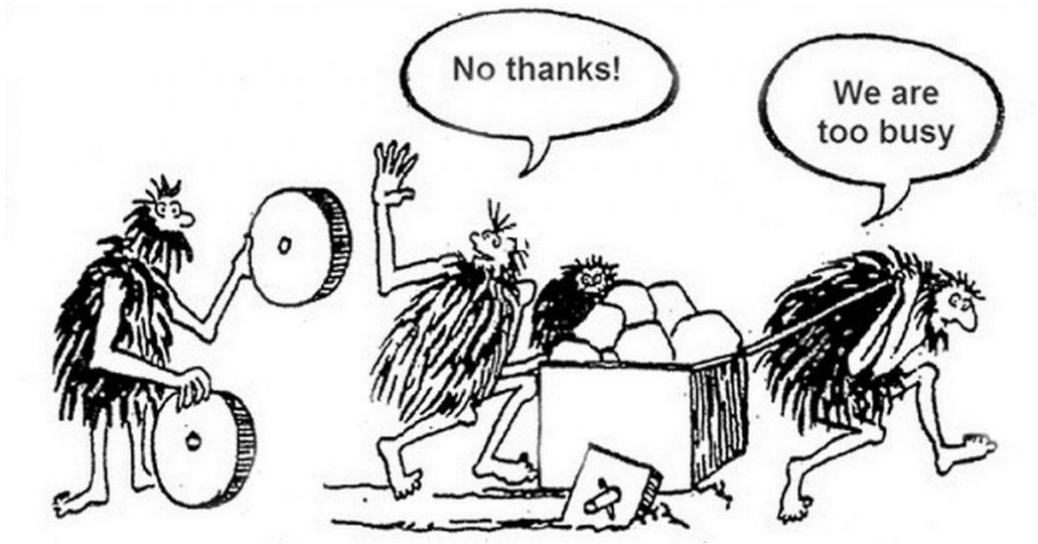
Relatiemanager Digital Trust Center

r.smaak@minezk.nl

06 2920 6573

Het DTC stelt ondernemend Nederland in staat om haar digitale veiligheid te vergroten.

Ondernemers die samenwerken maken meer mogelijk



WAAROM
MOEILIJK DOEN
ALS
HET SAMEN KAN

Loesje

Werken jullie al samen op het gebied van digitale veiligheid?

digital trust
center.

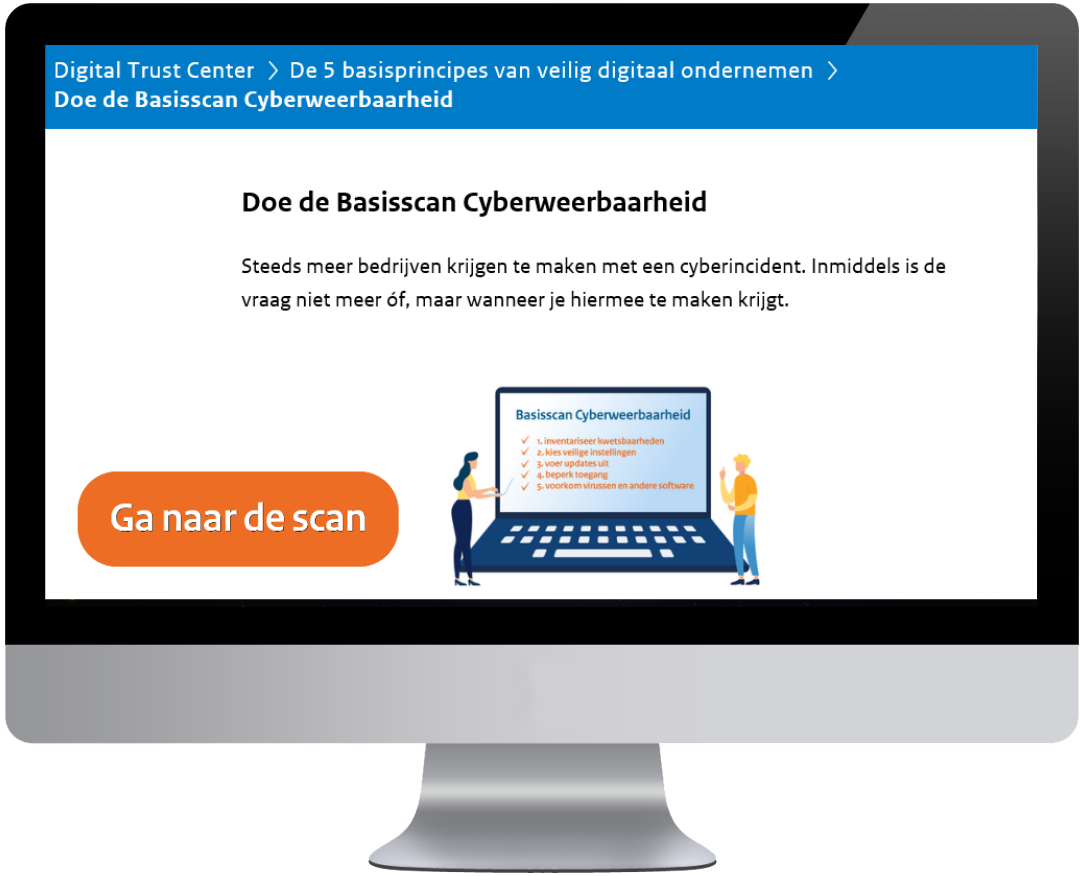
Het DTC kan helpen om ondernemers digitaal veiliger te maken

digital trust
center.

… door subsidie beschikbaar te stellen die samenwerking stimuleert

digital trust center.

… door onze kennis beschikbaar te stellen



digital trust center.

… door jullie te voorzien van specifieke informatie

digital trust center.

[TLP: WHITE] Reminder: deadline vervanging PKIoverheid-certificaten verloopt vandaag - Beri...

Bestand | Bericht | Help | Vertel wat u wilt doen

Verwijderen | Archiveren | Beantwoorden | Allen beantwoorden | Doorsturen | 03 Start-of-wee... | Aan manager | E-mail aan team | Verplaatsen | Labels | Bewerken | Spraak | In-/uitzoomen | Opslaan

wo 2-10-2019 12:34

dtcloket

[TLP: WHITE] Reminder: deadline vervanging PKIoverheid-certificaten verloopt vandaag

Aan

Cc Kolk, J.F. van der (Jacco); Veen, K.M. van der (Kim)

TLP: WHITE *Het is toegestaan deze informatie te delen met jullie aangesloten organisaties. Behoudens standaard copyrightregels, kan dit bericht zonder beperking worden verspreid. Zie de link voor meer informatie: https://first.org/tlp/*

Beste DTC partner,

Graag attenderen wij jullie op de reminder uitgebracht door het NCSC inzake de deadline vervanging PKIoverheid-certificaten die op 1 oktober is verlopen.

Dit betekent dat certificaten die nog niet vervangen zijn binnenkort ingetrokken zullen worden. Het intrekken van de certificaten zal leiden tot beschikbaarheidsproblemen.

In maart 2019 bleek dat een deel van de Public Key Infrastructure niet voldeed aan internationaal gestelde eisen. Getroffen certificaten moesten voor 1 oktober 2019 worden vervangen. Het NCSC informeerde u eerder over deze casus. [1]

Op dit moment is er nog niet op alle certificaten een reactie ontvangen. Het NCSC kan de impact van het intrekken van de certificaten en de daarbij behorende mogelijke beschikbaarheidsproblemen niet bepalen. Het NCSC adviseert om te reageren op de oproep van uw certificaatleverancier (TSP) om de getroffen PKIoverheidcertificaten in te trekken en/of te vervangen.

Het NCSC benadrukt het belang van veilig en wendbaar beheer van certificaten, zie de factsheet van het NCSC voor meer informatie. [2]

[1] https://www.ncsc.nl/actueel/nieuws/2019/september/6/deadline-vervanging-pkioverheid-certificaten-vervroegd-naar-1-oktober-2019
[2] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-veilig-beheer-van-digitale-certificaten

Met vriendelijke groeten,

Jacco van der Kolk & Kim van der Veen.
Relatiemanager Digital Trust Center (DTC)

M 06 25 64 25 12
E k.m.vanderveen@minezk.nl
W www.digitaltrustcenter.nl
.....
Ministerie van Economische Zaken en Klimaat
Bezuidenhoutseweg 73 | 2594 AC | Den Haag | D Passage 3
Postbus 20401 | 2500 EK | Den Haag
.....

Het Digital Trust Center stuurt deze nieuwsberichten naar de samenwerkingsverbanden omdat wij verwachten dat deze door jullie als nuttig ervaren worden. Mocht dit onverhoopt niet het geval zijn dan horen wij dat vanzelfsprekend graag. Mocht je de nieuwsberichten niet meer willen ontvangen dan volstaat een berichtje naar k.m.vanderveen@minezk.nl. Wij verwijderen uw

… door jullie toegang te geven tot de Digital Trust Community

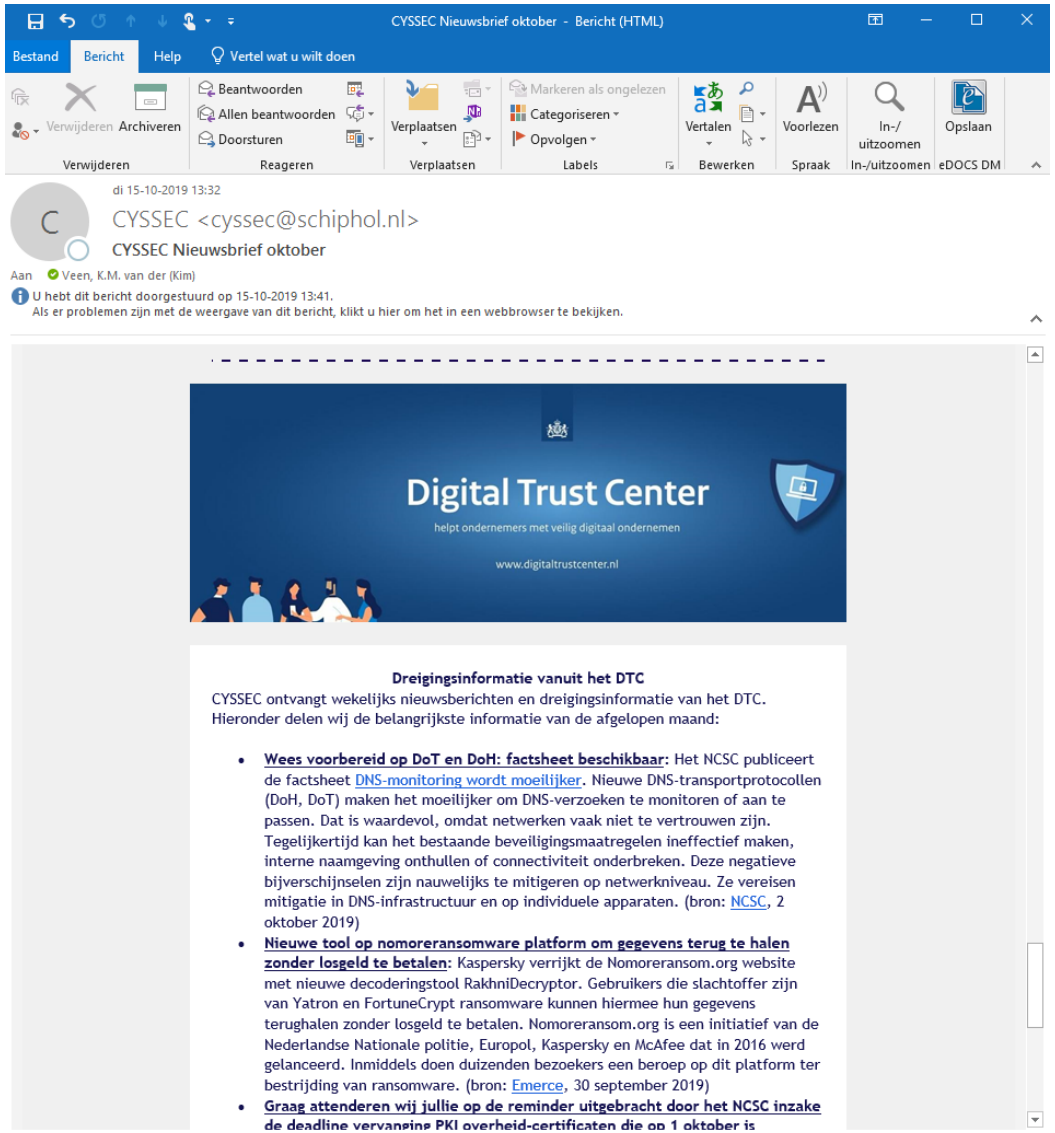
digital trust
center.

Waarom moeilijk doen als het samen kan?

digital trust
center.

Wat doen jullie op het gebied van digitale veiligheid?

digital trust center.



Ter inspiratie

Samenwerkingsverband CYSSEC

GEZOCHT: BEDRIJVEN DIE ETHISCH GEHACKT WILLEN WORDEN

CYBERSECURITY: DE BASIS OP ORDE

Ruim 40 procent van de bedrijven in de logistiek heeft wel eens te maken gehad met cybercriminaliteit. Volgens onderzoek van de Haagse Hogeschool zal dit in de toekomst vaker voorkomen.

Nederland is een logistieke hotspot met zijn geografische ligging en infrastructuur. Digitalisering is daarbij een belangrijke factor. Nederland moet daarom vooroplopen op het gebied van digitale security om nu en in de toekomst aantrekkelijk te blijven. Het Digital Trust Center (DTC) – een initiatief van het ministerie van Economische Zaken en Klimaat – kan hierbij helpen. Het DTC is er om het Nederlandse bedrijfsleven weerbaarder te maken tegen cyberdreigingen. Dit voorziet ondernemers van praktische informatie en advies via www.digitaltrustcenter.nl.

BASISPRINCIPES EN SCAN

Het DTC heeft vijf basisprincipes opgesteld die ondernemers helpen de basisbeveiliging voor veilig digitaal ondernemen op orde te krijgen. Ondernemers die deze basisprincipes opvolgen, vergroten hun weerbaarheid tegen cyberrisico's die de bedrijfsvoering kunnen verstoren. De basisprincipes zijn zo opgesteld dat iedere ondernemer, van zzp'er tot mkb'er, ermee uit de voeten kan. De maatregelen zijn toegankelijk en praktisch en staan opgesomd in illustratie bij dit artikel. Om ondernemers in korte tijd inzicht te geven in hun digitale veiligheid, kunnen zij ook gebruikmaken van een nieuwe cybersecurityscan die het DTC heeft ontwikkeld. Het is ook een goed middel om bedrijven aan te sporen tot het nemen van concrete acties om hun digitale weerbaarheid te vergroten. Met de 'basis op orde'-scan kunnen ondernemers direct aan de slag. Hiermee worden zij geholpen om inzicht te verkrijgen in waar de onderneming staat op het gebied van cybersecurity, maar de scan genereert naast praktische tips ook een uitgebreid adviesrapport over hoe een ondernemer de digitale veiligheid binnen zijn organisatie kan vergroten. De scan is te vinden op de website van het DTC: www.digitaltrustcenter.nl.

ONDERZOEK VIA HACK

Bedrijven kunnen ook op een andere manier hun digitale veiligheid vergroten, namelijk door mee te doen aan een zogenoemde ethische hack in het kader van een onderzoek door TNO samen met andere organisaties in de logistiek. Dit betreft een onderzoek naar de IT-security van bedrijven in de logistieke keten, dat moet leiden tot praktische handvatten voor logistieke bedrijven om de meest kritieke problemen in de keten te verhelpen en de cybersecurity te verbeteren. Het project wordt mede gefinancierd uit de Toeslag voor Topconsortia voor Kennis en Innovatie (TKI's) van het ministerie van Economische zaken. Voor het onderzoek is TNO op zoek naar logistieke bedrijven die zicht willen krijgen op hun IT-security via de uitvoering van een ethische hack – een gesimuleerde cyberaanval – door specialisten. Daarvoor is een tool in ontwikkeling die onderzoekt welke systemen door malware, bijvoorbeeld het 'WannaCry'-virus, aangetast kunnen worden. Deze tool, die bijna klaar is, wordt op het interne netwerk uitgevoerd. Vanzelfsprekend brengt de tool geen daadwerkelijke schade toe aan de systemen.

DE DOOR EEN ETHISCHE HACK VERWORVEN INFORMATIE KAN WORDEN GEBRUIKT OM DE SECURITY TE VERBETEREN

RESULTATEN

Na de ethische hack ontvangt het deelnemende bedrijf een overzicht van de resultaten. Het overzicht bevat ook een interpretatie van de resultaten om een duidelijk beeld te krijgen van de impact die een dergelijk incident op het interne netwerk kan hebben. De verworven informatie kan dus gebruikt worden om de security te verbeteren. Mogelijke uitkomsten zijn bijvoorbeeld dat de bestanden binnen het TMS niet meer beschikbaar zijn, er geen toegang meer is tot de vrachtbrieven of dat de voorraden in het voorraadsysteem niet meer inzichtelijk zijn.
De resultaten van de 'ethische hack' worden door TNO anoniem verwerkt voor het onderzoek dat het consortium met TNO uitvoert. Naast de 'ethische hack' neemt een TNO-medewerker een interview af om inzicht krijgen hoe de cybersecurity is georganiseerd.

PRAKTISCHE HANDVATTEN

De ethische hacks worden uitgevoerd door deskundige IT-securityspecialisten van Reqon Security. Zij ontwikkelen de tool en testen deze grondig. Uiteraard zijn zij bereid om een geheimhoudingsverklaring (NDA) te ondertekenen. Dat geldt ook voor de

Ter inspiratie

Brancheorganisatie Transport Logistiek Nederland

Ter inspiratie

Brancheorganisatie Adfiz

Hoe kan het DTC jullie verder helpen om ondernemers digitaal weerbaarder te maken?

digital trust
center.

Vragen???

Rajko Smaak
Relatiemanager DTC
r.smaak@minezk.nl
06 2920 6573

digital trust center.