Ministerie van Economische Zaken
en Klimaat

Terugblik
Digital Trust Center 2021

Terugkijken naar het jaar, samenwerken aan de toekomst

Voorwoord

In het Regeerakkoord ‘Omzien naar elkaar, vooruitkijken naar de toekomst’ is expliciet melding gemaakt van het DTC. Het nieuwe kabinet ziet voor het DTC een rol weggelegd om in samenwerking met andere organisaties zoals NCSC, “sneller en makkelijker informatie (te) delen over digitale kwetsbaarheden en hacks”.

Als variant op de titel van het Regeerakkoord wil ik voor dit jaarbericht als titel hanteren “terugkijken op het jaar, samenwerken aan de toekomst”. Een toekomst die ons dichter brengt bij een cyberweerbaar ondernemend Nederland. De activiteiten en producten van het DTC van het afgelopen jaar hebben volgens mij hierbij geholpen. Als we terugblikken naar de resultaten van het einde van het jaar, mogen we best tevreden zijn.

Alle doelstellingen zijn gerealiseerd, soms zelfs ruim overtroffen. Het bereik is sterk toegenomen wat te zien is aan een aanzienlijke groei in aantal bezoekers van de website (meer dan 225.000 in 2021), de lancering en veelvuldig gebruik van nieuwe tools en de doorbraak van de DTC-community in het laatste kwartaal van 2021. Ook het aantal samenwerkingsverbanden nam met zeven toe en de interactie werd vergroot door periodieke ontmoetingen. Helaas online.
Daarbij heeft de lancering van een nieuwe dienst, het notificeren van individuele bedrijven over kwetsbaarheden waar de overheid weet van heeft, een goede start en ontvangst gekregen. In de pers en de politiek maar belangrijker nog bij de ondernemers die de verkregen dreigingsinformatie meestal dankbaar ontvingen en ermee aan de slag gingen.

Dus tevredenheid over wat er is bereikt. In het besef dat we dit alleen hebben kunnen realiseren met de hulp van stakeholders als VNO-NCW/MKB-Nederland, NLdigital, CIO-platform, KvK en ECP, onze samenwerkingsverbanden en partners als NCSC en DIVD. Voor het komend jaar gaan we er weer met volle kracht tegen aan. Met extra mensen en met nieuwe energie gaan we de lat nog hoger leggen.

Onze doelgroep is enorm gevarieerd en talrijk en ook de cyberincidenten lijken alleen maar toe te nemen. Dus weer samen aan de slag!

Michel Verhagen
Manager Digital Trust Center

Inhoud

Het jaar in cijfers

Het Digital Trust Center (DTC) heeft het afgelopen jaar weer grote stappen gezet om de digitale veiligheid van ondernemend Nederland te vergroten. Onze doelgroep van circa 2 miljoen ondernemers in de zogenaamde 'niet vitale' sectoren is zeer uiteenlopend. Van zzp'ers tot het grootbedrijf. Maar wat ze allemaal gemeen hebben, is dat ze steeds meer te maken krijgen met digitalisering en cyberrisico's.

Mede door corona hebben we de afgelopen twee jaar een stroomversnelling gezien in de digitalisering van de samenleving. Dit draagt bij aan een open, vrije en innovatieve samenleving. Maar het is tegelijkertijd ook een kans voor cybercriminelen om hun slag te slaan. Want helaas groeit de cyberweerbaarheid van bedrijven niet met gelijke voet mee met de digitale ontwikkelingen.
In 2021 heeft het DTC de nadruk gelegd op het zowel proactief als reactief de cyberweerbaarheid van ondernemend Nederland vergroten.

DTC heeft ook het nodige gedaan aan preventie van schade door cyberaanvallen. Er zijn extra samenwerkingsverbanden gecreëerd om sectoraal of regionaal cyberinitiatieven te ontplooien. Ook weten in toenemende mate ondernemers hun weg te vinden naar de begrijpelijke informatie over te nemen cybermaatregelen ter verhoging van de cyberweerbaarheid.

227.123
Website bezoeken

6.796
Social media volgers

739
Deelnemers community

37
Samenwerkingsverbanden

6
Projecten geselecteerd voor subsidieregeling cyberweerbaarheid

99
Nieuwe content pagina's op DTC website

Actief informeren over cyberdreigingen

Het DTC ziet het als taak om ondernemers op de hoogte te stellen van ernstige cyberdreigingen. In voorgaande jaren gaven we alleen invulling aan deze taak door alerts te versturen over algemene ernstige dreigingsinformatie.

Halverwege 2021 is daar een extra mogelijkheid bijgekomen. Afgelopen zomer hebben we de OKTT-status (Objectief Kenbaar Tot Taak) verkregen. Daardoor kan het Nationaal Cyber Security Centrum (NCSC) specifieke dreigingsinformatie met het DTC delen. Met deze informatie benaderen we sinds september bedrijven proactief over digitale dreigingen. Onze informatiedienst heeft in 2021 ruim 350 ondernemers gericht kunnen waarschuwen over ernstige dreigingen. Deze bedrijven konden hierdoor op hun beurt maatregelen nemen om de schade te voorkomen of te beperken. Het DTC geeft waar mogelijk advies over te nemen maatregelen, zoals het installeren van beveiligingsupdates, het aanpassen van wachtwoorden of het inschakelen van een IT-specialist.

Pilot 'gevraagd notificeren'

Er zijn ook cyberdreigingen die duizenden bedrijven tegelijkertijd kunnen raken. Om zoveel bedrijven op tijd te kunnen waarschuwen, onderzoeken we de schaalbaarheid van onze dienstverlening. We zijn daarom ook gestart met het inrichten van de pilot 'gevraagd notificeren'. In deze pilot onderzoeken we gedurende 12 maanden of en hoe we de 'waarschuwingsdienst' kunnen automatiseren. De 57 bedrijven die deelnemen aan de pilot vertegenwoordigen diverse sectoren. Daardoor is er een goede afspiegeling van het bedrijfsleven.

Het waarschuwen werkt op basis van automatische matching. De pilot deelnemers hebben bedrijfstechnische gegevens met ons gedeeld. Als wij informatie over dreigingen ontvangen, kunnen we daardoor direct de relevante pilotdeelnemers op de hoogte stellen. De resultaten van de pilot zullen in de loop van komend jaar bepalen hoe we deze dienst verder invullen.

Mijlpalen

- **Zomer 2021 krijgt het DTC de OKTT status toegewezen**
- **26 cyber alerts gepubliceerd over algemene ernstige dreigingsinformatie**
- **361 bedrijven genotificeerd over bedrijfsspecifieke ernstige dreigingen**
- **57 deelnemers aan de pilot 'gevraagd notificeren'**

Sinds we de OKTT-status hebben, ontvingen meer dan 350 bedrijven het afgelopen jaar een telefoontje of mailtje van ons over een kwetsbaarheid in hun bedrijfssoftware of systeem. Deze kwetsbaarheden werden vaak veroorzaakt door een server of bedrijfssoftware waar een beveiligingslek in zat. Dit kan schadelijke gevolgen hebben, zoals een ransomware-aanval of diefstal van bedrijfsgegevens.

We kunnen moeilijk vaststellen of er dankzij onze waarschuwingen daadwerkelijk schade voorkomen is. Bedrijven zijn uiteraard niet verplicht om de adviezen over te nemen. Maar uit enkele reacties valt op te maken dat er opvolging aan gegeven werd. Soms is er nog verbazing bij ontvangers van de urgente boodschap, omdat het DTC nog niet bij iedereen bekend is.

DTC samenwerkingsverbanden groeit naar 37

Cyberheroes | Cyberweerbaarheid Noord Nederland | Groep Educatieve Uitgeverijen | Cybersecurity Programma Noordzeekanaalgebied | Cyberweerbaarheid In De Agrarische Sector | Stichting Nederlandse Industrie Voor Defensie En Veiligheid | Cybersecurity Synergie Schiphol Ecosysteem | Cybersecurity Center Maakindustrie | Cyberchain | Nationale Beheersorganisatie Internetproviders | Connect2trust | Techniek Nederland | Brainport | Nubedrijfsnoodorganisatie | Thuiswinkel.org | Zorgcert | Adfiz | Cyberweerbaarheid In Limburg | Agrifood | Cyberweerbaarheid | Noordelijke Productiviteits Alliantie | Cybernetwerk Zuid Hollandse Eilanden | Noord Holland Samen Veilig | Hi Cybersecurity Network | Platform Zelfstandig Ondernemers | Cyberweerbaarheid Groentezaadveredelingsbedrijven | Cyberweerbaarheids-netwerk Drechtsteden | Bouwend Nederland | Transport En Logistiek Nederland | Ferm Rotterdam | Federatie Van Technologiebranches

Nieuw In 2021: Dutch Institute For Vulnerability Disclosure (Divd) | Nationale Anti-ddos-coalitie | Cyberweerbaarheidscentrum Greenport West-holland | Mmox: Netwerk Voor Risk-based Cyberweerbaarheid (Nrbc) | Synanta Bv: Mkb Cybersecurity Governance | Stichting Cyber Safety Noord Nederland

Bouwnijverheid Defensie E-commerce financieel Haven Hightech industrie IT Landbouw Luchtvaart Non-profit Onderwijs Overheid Retail Techniek Zorg

Samenwerken aan een cyberweerbaar Nederland

Twee miljoen ondernemers is een grote doelgroep. Uiteraard kunnen we niet zoveel ondernemers alleen bereiken. We bouwen aan een landelijk dekkend stelsel van cyberweerbaarheidsnetwerken. Binnen dit stelsel kan informatie over cybersecurity breder, efficiënter en effectiever worden gedeeld tussen publieke en private partijen. Op die manier kunnen we gezamenlijk de slagkracht vergroten. In 2021 heeft het DTC 6 nieuwe samenwerkingsverbanden verwelkomd. Daarmee is het totale aantal cyberweerbaarheidsnetwerken binnen ons landelijk dekkend stelsel dit jaar op 37 uitgekomen.

Het DTC heeft afgelopen jaar de samenwerking met het Nationaal Cyber Security Centrum (NCSC) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) versterkt. Op operationeel en strategisch niveau werkten we dit jaar nauw samen met het NCSC om de dreigingsinformatie-dienst neer te zetten. Met het NCTV hebben we de banden aangehaald om het landelijk dekkend stelsel meer vorm te geven. Zo is er bij de Log4j-kwetsbaarheid intensief samengewerkt om in korte tijd zoveel mogelijk ondernemers en IT-specialisten op de hoogte te brengen van de ernst, omvang en te nemen maatregelen om deze situatie meester te worden.

Sinds enkele jaren wordt er in de maand oktober in heel Europa extra aandacht besteed aan het onderwerp cybersecurity. Het is een belangrijk moment waarop de Nederlandse cyberwereld tijdens diverse evenementen bijeenkomt. Het jaarlijkse hoogtepunt is de ONE Conference in Den Haag. Dit jaar heeft het DTC daar de samenwerking opgezocht door bij te dragen aan presentaties en artikelen.

Een mooie kans voor brancheverenigingen

Het DTC organiseerde eind november een webinar speciaal voor brancheverenigingen. Nicole Mallens, beleidssecretaris van VNO-NCW, sprak daar over het belang van cybersecurity voor het Nederlandse bedrijfsleven: ‘Onze maatschappij is steeds verder gedigitaliseerd, en datzelfde geldt voor bedrijven. Bedrijven kunnen tegenwoordig niet meer zonder hun digitale systemen. Tegelijkertijd zie je dat cybercriminelen steeds actiever worden, dit heeft vaak grote schade tot gevolg. Bedrijven nemen stappen, vanuit zichzelf, of vanuit de keten. Maar veel bedrijven vinden het erg ingewikkeld of schatten de kans dat zij slacht-offer worden niet hoog in. Alle bedrijven zijn kwetsbaar voor cybercriminaliteit. Digitalisering en digitale veiligheid moeten hand in hand gaan.’

Via samenwerkingsverbanden probeert het DTC brancheorganisaties zoveel mogelijk te betrekken in de missie om Nederland digitaal veiliger te maken. Ze zijn van grote waarde, zegt Nicole: ‘Brancheorganisaties kunnen een heel belangrijke rol spelen om de digitale weerbaar-heid van ondernemend Nederland te vergroten. Dat kwam ook uit eerdere onderzoeken die zijn gedaan op dit terrein. Voor bedrijven is de brancheorganisatie een vertrouwde omgeving en de informatie die via een branche komt wordt door bedrijven goed ontvangen. Brancheorganisaties zijn van, voor en door ondernemers. Ik zie dat er al brancheorganisaties zijn die stappen zetten om hun leden te informeren. Ik hoop dat meer brancheorganisaties hun voorbeeld gaan volgen.’

Educatie en voorlichting

Een cyberweerbaar Nederland begint bij een goede kennisbasis. Het DTC biedt daarom laagdrempelige kennis, informatie en advies over een breed scala aan onderwerpen gerelateerd aan cyberweerbaarheid.

Lancering twee nieuwe interactieve tools

De Risicoklassenindeling Digitale Veiligheid is speciaal ontwikkeld voor het midden- en kleinbedrijf. Aan de hand van 11 vragen wordt een inschatting gemaakt hoe groot het risico is op een cyberincident. Deze inschatting bepaalt in welke risicoklasse een onderneming valt en welke maatregelen er genomen moeten worden om digitale veiligheid te borgen.

Met de Security Check Procesautomatisering kunnen organisaties snel in kaart brengen waar mogelijke risico's zitten in het gebruik van OT of ICS techniek, maar ook welke beschermingsmaatregelen zij hiertegen kunnen nemen. De bedrijfsvoering van de meeste organisaties is tegenwoordig, vaak zonder dat ze zich daarvan bewust zijn, sterk afhankelijk van automatiserings- en control systemen. Deze zelfscan, die ook zonder technische of IT-kennis kan worden gebruikt, biedt organisaties een praktisch hulpmiddel om hun cyberweerbaarheid te vergroten. De Security Check Procesautomatisering is feestelijk gelanceerd in juli. Deze interactieve zelfscan is ontwikkeld door een breed publiek-privaat samenwerkingscollectief op het gebied van cyberveiligheid in operationele techniek (OT).

Actief in gesprek met de doelgroep

In 2021 hadden we ook een duidelijke focus om actief het gesprek aan te gaan met ondernemend Nederland. Ondanks de coronamaatregelen, die fysieke ontmoetingen een groot deel van het jaar niet mogelijk maakte, zochten we door middel van webinars, workshops, presentaties en via social media kanalen het contact op met ondernemers. De doorontwikkeling van de DTC Community (zie pagina 9) speelt daarbij een belangrijke rol.

Het afgelopen jaar hebben we ons ook ingezet om onze naamsbekendheid en vindbaarheid te vergroten. Zo zijn we gaan samenwerken met brancheorganisaties die eenzelfde doel hebben: digitale veiligheid vergroten. Brancheorganisaties zijn van, voor en door ondernemers. Zij kunnen een belangrijke rol spelen bij het informeren van hun leden over dit vaak ingewikkelde thema.

In november organiseerden we een webinar speciaal voor IT-dienstverleners met medewerking van NLdigital. VNO-NCW en MKB-Nederland werkten mee aan een webinar speciaal voor brancheorganisaties. In beide informatiesessies werd op praktische wijze aandacht besteed aan vragen als: Hoe maak je leden van je organisatie bewust over cybergevaren? Hoe informeer je ze over te nemen maatregelen? Hoe worden bedrijven op de hoogte gesteld van cyberdreigingen?

Benieuwd naar deze informatiesessies? Beide webinars zijn terug te kijken via ons YouTube-kanaal.

Mijlpalen

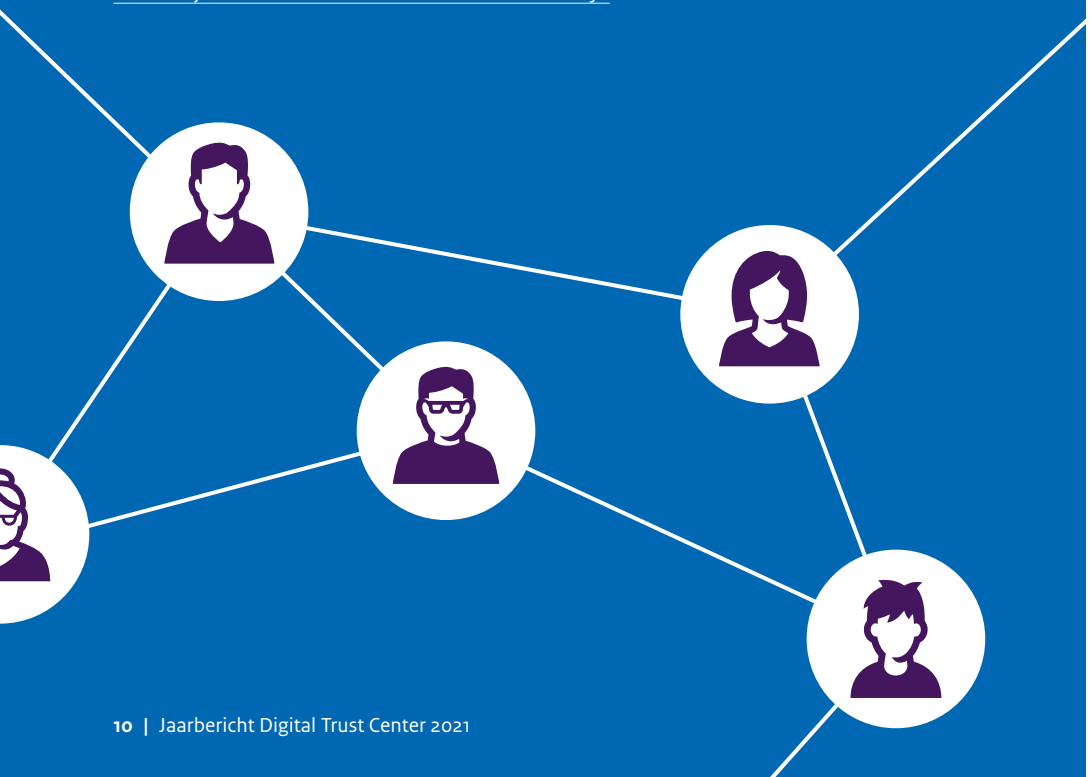
- **Livegang tool Security Check Procesautomatisering**
- **Livegang tool Risicoklassenindeling**
- **99 blogposts en artikelen gepubliceerd**
- **739 leden DTC community**
- **28 webinars, workshops en presentaties**
- **225.000 bezoeken DTC website**

De DTC community

De DTC Community biedt aangesloten leden de mogelijkheid om, in een besloten omgeving, actuele en relevante informatie over cybersecurity uit te wisselen. Ook verspreidt het DTC via dit kanaal urgente dreigingsinformatie. Zo kunnen we samen de kans op misbruik door cybercriminelen verkleinen.

De DTC Community is met meer dan 700 Nederlandse ondernemers en IT-, ICT- of cybersecurity verantwoordelijken uit verschillende branches in 2021 een belangrijk platform geworden.
Door je als ondernemer aan te sluiten bij de DTC Community vergroot je de digitale weerbaarheid van jouw organisatie en draag je bij aan een veiliger ondernemersklimaat in de keten én in heel Nederland. Want via informatie-uitwisseling vergroten we gezamenlijk onze weerbaarheid tegen cybercriminaliteit.

Zien we jou binnenkort ook in de DTC Community?



Oktober cybersecurity maand

Relatiemanager Jacco van der Kolk blikt terug op de cybersecurity maand.

Heel veel dingen liepen door corona de afgelopen twee jaar anders dan gepland. Maar gelukkig was oktober gewoon weer de European Cyber Security Month. Oktober staat daarmee in het teken van het creëren van bewustwording op het gebied van online veiligheid, het stimuleren van veilig gedrag online en aandacht vragen voor actuele cybergevaren en het vergroten van cyberveiligheid.

Er worden in Europa, en zeker in Nederland, jaarlijks tal van conferenties, webinars en trainingen georganiseerd. Maar de ONE steekt er wat mij betreft echt met kop en schouders bovenuit. De conferentie vond dit jaar plaats in de laatste week van september en was daarmee de perfecte aftrap van de European Cyber Security Maand.

De conferentie had een hybride vorm. Een aantal deelnemers mocht er fysiek bij zijn. De rest kon via internet meedoen. Het was voor mij persoonlijk heel prettig om er fysiek bij te zijn. Het was goed om contacten weer in levende lijve te ontmoeten. Ik heb vele interessante lezingen bijgewoond en zelf een lezing gehouden over onze nieuwe beveiligingstool voor Industrial Control Systemen (ICS).

Verder heb ik natuurlijk veel webinars gevolgd. Er waren er heel veel, maar een kleine greep uit het aanbod: de online Kick-off van Alert Online, een aantal verschillende webinars van Weerbare Digitale Overheid, de webinar over cyberfraude van het Verbond van Verzekeraars en een masterclass over ethiek van het Centrum Informatiebeveiliging en Privacybescherming.

Het is fantastisch om te zien dat er zoveel georganiseerd wordt. Zelfs als het fysiek niet altijd mogelijk is!’

Cyberweerbaarheid van ondernemend Nederland in beeld

De data die we verkrijgen via onze tools, zoals de Basisscan Cyberweerbaarheid, zijn van grote waarde voor ons. We halen hier belangrijke inzichten uit die ons verder kunnen helpen met onze missie om Nederland digitaal weerbaarder te maken. Maar we vinden kwalitatieve interactie ook belangrijk: we gaan graag in gesprek met ondernemers om ze beter te leren kennen en te begrijpen.

De basisscan is in de afgelopen jaren ruim 4000 keer volledig ingevuld op de DTC-website. Voor de cijfers in de komende alinea's zijn we uitgegaan van ruim 1000 volledig ingevulde scans in 2021. De cijfers geven slechts een indicatie en worden daarom telkens met CBS-cijfers vergeleken.

De 5 Basisprincipes

Het DTC heeft de 5 basisprincipes van veilig digitaal ondernemen opgesteld om ondernemers te helpen met hun cyberweerbaarheid. Ondernemers die deze basisprincipes volgen, vergroten hun weerbaarheid tegen cyberrisico's die de bedrijfsvoering kunnen verstoren. Ze zijn zo opgesteld dat iedere ondernemer - van zzp'er tot mkb'er - ermee uit de voeten kan. Aan de hand van deze principes lichten we een aantal opvallende incidenten en ontwikkelingen van afgelopen jaar uit. Wat kunnen we hiervan leren en wat is de verwachting voor 2022? Deze inzichten zijn mede gebaseerd op gegevens uit onze Basisscan Cyberweerbaarheid en de CBS Cybersecuritymonitor.

Basisprincipe 1: Inventariseer kwetsbaarheden

Het afgelopen jaar stond grotendeels in het teken van ransomware. Er is haast geen week voorbij gegaan zonder nieuws over nieuwe ransomware-aanvallen, gericht op grote én kleinere bedrijven. Bij ransomware worden computers of de bestanden erop gekaapt en vervolgens versleuteld waardoor ze niet meer toegankelijk zijn. De criminelen laten het slachtoffer daarna een losgeldbedrag ('ransom') betalen om weer toegang te krijgen tot de versleutelde bestanden.

Het DTC raadt af om losgeld te betalen. Dat houdt het probleem van ransomware in stand en het is niet altijd gezegd dat je ook echt je bestanden terugkrijgt. Een belangrijk advies om de schade van ransomware te beperken, is het regelmatig maken van goede back-ups van je bestanden.

Uit de Basisscan Cyberweerbaarheid blijkt dat 74% van de ondernemers regelmatig een back-up maakt van alle belangrijke informatie binnen het bedrijf. Dat betekent dat nog zo'n 1 op de 3 ondernemers nog géén goede back-up routine heeft ingericht.

De CBS cybersecuritymonitor geeft de afgelopen jaren overeenkomstige percentages. 2019: 72%, 2020: 71%

Basisprincipe 2: Kies veilige instellingen

Geregeld komen er lijsten voorbij met de meest gebruikte wachtwoorden van dat moment. Wachtwoorden als ''123456'' en ''qwerty'' blijven de top 5 aanvoeren. **Uit de Basisscan Cyberweerbaarheid blijkt dat 63% van de ondernemers zeker weet dat er verschillende, complexe, wachtwoorden zijn ingesteld om apparaten en bedrijfsgegevens te gebruiken.**

Er is nog veel ruimte voor verbetering op het gebied van wachtwoordbeleid. Een streng wachtwoordbeleid is een concrete maatregel die valt onder basisprincipe 2: kies veilige instellingen.

Ook de CBS cybersecuritymonitor meldt het percentage bedrijven met een beleid voor sterke wachtwoorden. 2019: 65%, 2020: 68%

Basisprincipe 3: Voer updates uit

In 2021 werden er meerdere kwetsbaarheden ontdekt binnen Microsoft Exchange Server waarmee zo'n server volledig kon worden overgenomen door een kwaadwillende. Microsoft bracht hiervoor beveiligingsupdates uit om de kwetsbaarheid op te lossen. Het advies in deze situatie valt terug op Basisprincipe 3: voer je updates uit.

Het Amerikaanse Joint Cybersecurity Advisory stelde dat de meest misbruikte kwetsbaarheden van het afgelopen jaar bekende - en vaak gedateerde - kwetsbaarheden zijn. Tijdig updaten van alle apparaten die verbonden zijn met het netwerk is cruciaal. Updaten voorkomt namelijk dat verouderde software misbruikt kan worden door cybercriminelen.

Uit de cijfers van de Basisscan Cyberweerbaarheid blijkt dat in 2021 bijna 82% van de ondernemers zeker wist dat alle software binnen het bedrijf waren voorzien van de laatste updates. Hieruit kunnen we opmaken dat veel ondernemers op de goede weg zijn, maar dat er nog werk aan de winkel is.

Deze cijfers zijn in lijn met de cijfers die het CBS in haar cybersecuritymonitor publiceerde.
2019: 81%, 2020: 84%

Basisprincipe 4: Beperk toegang

Een ander opvallend incident is een gelekte lijst met een grote hoeveelheid Fortinet VPN-gebruikersnamen en wachtwoorden. Met deze VPN-inloggegevens kan een crimineel netwerktoegang krijgen en vervolgens kwaadaardige software installeren, data stelen of (gerichte) ransomware-aanvallen uitvoeren. In het geval van een gelekte lijst met wachtwoorden en gebruikersnamen is het belangrijk om zo spoedig mogelijk nieuwe, sterke wachtwoorden in te stellen. Het advies is ook om altijd tweefactorauthenticatie (2FA) in te stellen. Deze concrete maatregel komt voort uit basisprincipe 4: beperk toegang. 2FA voegt een tweede veiligheidslaag toe aan de toegangsvereisten van een systeem of applicatie. Alleen een gebruikersnaam en wachtwoord is daardoor onvoldoende om toegang te krijgen.
Uit de Basisscan Cyberweerbaarheid blijkt dat slechts 55% van de ondernemers in 2021 naast een wachtwoord een extra vorm van authenticatie hebben ingesteld.

In de CBS cybersecuritymonitor is dit percentage zelfs lager.
2019: 39%, 2020: 46%

Basisprincipe 5: Voorkom virussen en andere malware

Als laatste richten we ons op basisprincipe 5: voorkom virussen en andere malware. Er zijn verschillende manieren om je te beschermen tegen malware en virussen. Een veelgebruikte methode is antivirus software. **Volgens de Basisscan Cyberweerbaarheid gebruikt 75% van de ondernemers antivirus software op alle bedrijfsapparatuur.** Een andere belangrijke manier om virussen en malware te voorkomen is door veilig gedrag van medewerkers te stimuleren. De cyberweerbaarheid van je bedrijf valt of staat met het gedrag van medewerkers. Prikkel daarom continu de alertheid voor cybersecurity, wacht niet tot het te laat is!

Het CBS deelt zelfs een percentage van 89% van de ondernemers in 2019 en 2020.

Terugblik op de Log4j problematiek

Begin december 2021 dook misschien wel de ernstigste kwetsbaarheid van het hele jaar op.

Je hebt het vast op onze website of andere media-kanalen voorbij zien komen toen half december een kwetsbaarheid werd aangetroffen in Apache log4j. Log4j is een veel gebruikte open source bibliotheek die vooral door softwareontwikkelaars wordt gebruikt om te loggen. Een groot deel van het bedrijfsleven maakt gebruik van software waar Log4j in verwerkt zit. Zij kunnen daarom afhankelijk zijn van updates van hun softwareleverancier die op hun beurt de (Apache) Log4j updates dienen te verwerken in hun software. Daarnaast hebben bedrijven vaak een externe IT-dienstverlener die gebruikte software binnen de organisatie beheert. Dit houdt in dat deze ondernemers niet direct zelf de nodige updates kunnen uitvoeren en niet weten voor welke gebruikte software dat nodig is.

In de uren die volgden na deze eerste melding is er een hoop gebeurd. Het NCSC lanceerde een Github-pagina waarop een lijst wordt bijgehouden met applicaties die kwetsbaar zijn als gevolg van de kwetsbaarheid. In de tussentijd werden door Apache verschillende updates beschikbaar gemaakt, waarbij het telkens van groot belang was om zo snel mogelijk te updaten.

Werk aan de winkel dus, zowel voor organisaties als het DTC en het NCSC als voor Nederlandse bedrijven. Het was in deze periode cruciaal om zo veel mogelijk mensen te informeren over de kwetsbaarheid in Log4j, en hen te helpen bij het nemen van mitigerende maatregelen. In samenwerking met het NCSC organiseerde het DTC daarom een IT-informatiesessie over de kwetsbaarheid Log4j. In een livestream van 45 minuten werd door verschillende experts van het NCSC en het DTC de problematiek rondom deze kwetsbaarheid geduid. Daarnaast was er de mogelijkheid om vragen te stellen. Dit webinar is bezocht door meer dan 4000 ondernemers en cyberprofessionals.

Meer weten over deze sessie, of de sessie terugkijken? Kijk hier.

Verhalen uit de praktijk

Het DTC gaat regelmatig in gesprek met ondernemers die slachtoffer zijn geworden van een cyberaanval of -incident. Alhoewel lang niet iedereen hier graag over praat, zijn er wel degelijk ondernemers die hun ervaringsverhaal willen delen.

We horen dat veel ondernemers cyberweerbaarheid steeds meer als een onderdeel van hun bedrijfsvoering gaan zien. Dat is goed nieuws. Helaas blijven er ook nog veel ondernemers achter. Er zijn nog veel bedrijven die pas hun basisprincipes op orde brengen op het moment dat het te laat is.

Veel ondernemers die we spreken geven aan dat ze het moeilijk vinden aangifte te doen. Ze hebben geen tijd voor een aangifte op het politiebureau en hebben het gevoel dat er niks mee gedaan wordt.

Ondernemers kenden het DTC vaak (nog) niet. Ze juichen het toe dat het bestaat, maar een veelgehoord advies is om de communicatie meer via de brancheverenigingen en KVK te laten lopen.

Hightech bedrijf uit Schiedam is goed voorbereid

Boers & Co Precision Solutions is een bedrijf in Schiedam dat hightech onderdelen en apparaten ontwerpt en produceert. Het bedrijf is zo afhankelijk van computers en data, dat het geen enkel risico neemt op het gebied van cyber. Ze hebben een geavanceerd back-upsysteem en doen veel aan bewustwording bij de medewerkers.

En zelfs dan kan het misgaan. Hoort bij het vak, zegt CEO Ronald Koot: ‘Je bent nooit 100% veilig. Het gaat elke ondernemer hoe dan ook een keer overkomen dat hij of zij gehackt wordt. De vraag is alleen: wanneer?’

De laatste keer dat Boers & Co getroffen werd, was in 2017, vertelt Ronald. ‘Een van onze werknemers opende een bijlage met een virus. Binnen enkele seconden waren alle bestanden op ons netwerk besmet. Ontwerptekeningen, contracten, technische informatie. Alles. Die medewerker wist gelijk dat het fout zat en heeft direct een melding gedaan. Daardoor konden we heel snel in actie komen. Een paar uur later waren we weer up en running.’

Sinds die laatste cyberaanval heeft Ronald Koot aanvullende beveiligingsmaatregelen genomen. Dat betekent in sommige gevallen meer werk voor zijn medewerkers, maar de veiligheid staat voorop.

Lees het hele verhaal over Boers & Co

Colofon

DTC Terugblik
Editie 1 Jaargang 2021

Publicatiedatum
03 februari 2022

Hoofdredactie
Digital Trust Center

Productie
Digital Trust Center

Vormgeving
Digital Trust Center

website
www.digitaltrustcenter.nl

Redactieadres
Postbus 20401 2500 EK Den Haag

Volg ons via: