De reacties van bedrijven

De 43 bedrijven en organisaties die hun mailservers niet optimaal hebben beveiligd, zijn ruim voor de uitzending hiervan op de hoogte gesteld, zodat ze alsnog passende maatregelen konden nemen. Zembla heeft hen ook ter wederhoor om een reactie gevraagd.

Onze vragen:
Het tv-programma Zembla (BNNVARA) bereidt een uitzending voor over de cyberveiligheid van Nederland die op 7 oktober te zien is op NPO2. Voor deze uitzending heeft Zembla samen met onafhankelijke onderzoekers van Stichting Internet CleanUp Foundation een veiligheidscheck gedaan bij organisaties en bedrijven die van vitaal belang zijn voor Nederland. Daarbij is gekeken welke veiligheidsmaatregelen er zijn genomen op de mailservers.

Uit de screening van Zembla en Stichting Internet CleanUp Foundation blijkt dat uw mailserver (@xxxxx.nl) niet aan één of meerdere van de belangrijkste internetveiligheidsstandaarden voldoet. Het gaat dan om DKIM (RFC6376), SPF (RFC7208) en DMARC (RFC7489). In uw geval ontbreekt SPF/DKIM/DMARC en/of is het DMARC-beleid onvoldoende strikt ingesteld.

Uw organisatie is hierdoor volgens de onderzoekers onnodig kwetsbaar voor cybercriminaliteit, zoals mailspoofing, CEO-fraude, spearphishing en ransomware. Ook het Nationaal Cyber Security Center waarschuwt in diverse factsheets en adviezen voor het ontbreken hiervan. Deze kwetsbaarheid maakt het voor cybercriminelen bijvoorbeeld makkelijk om zich voor te doen als xxxxx-medewerker of zelfs als directielid, waardoor zij vanuit diens naam met diens authentieke e-mailadres een mail kunnen versturen aan derden. Dit is niet alleen een theoretische situatie, aangezien er in Nederland al regelmatig van deze vorm van fraude gebruik is gemaakt.

Op basis van deze bevindingen, zouden we graag willen weten:

1. *Kunt u aangeven waarom betreffende veiligheidsmaatregel (SPF/DKIM/DMARC, met strikte policy) niet is genomen?*

2. *Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?*

3. *Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)*

4. *Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?*

5. *Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?*

6. *Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?*

7. *Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?*

De antwoorden van de bedrijven vindt u hieronder, op alfabetische volgorde.

1. Arriva
2. ASN Bank
3. Centraal Orgaan Voorraadvorming Aardolieproducten
4. Coteq
5. DB Cargo Nederland
6. Dunea
7. Enduris
8. Enexis
9. Engie
10. EPZ (exploitant kerncentrale Borssele)
11. Essent
12. Euronext
13. Evides
14. KLM
15. Luchtverkeersleiding Nederland
16. Nederlandse Aardolie Maatschappij
17. PWN / Drinkwater Noord Holland
18. Reactor Instituut Delft
19. RWE
20. Schiphol
21. Stedin
22. Tennet
23. T-Mobile
24. Uniper
25. Vattenfall
26-38. Veiligheidsregio's Amsterdam, Brabant-Noord, Friesland, Gelderland-Midden, Gelderland-Zuid, Groningen, IJsselland, Limburg-Noord, Midden- en West-Brabant, Rotterdam-Rijnmond, Utrecht, Zeeland en Zuid-Limburg
39. Vodafone Ziggo
40. Waterbedrijf Groningen
41. Westland Infra / Juva
42. WMD / Drinkwater Drenthe
43. WML / Drinkwater Limburg

1. Arriva

In de afgelopen vijf jaar zijn er in relatie tot Arriva Nederland enkele pogingen tot CEO-fraude en reguliere phishingmails gedaan. Deze pogingen waren niet succesvol en Arriva is als organisatie nooit door het NCSC actief benaderd of gewaarschuwd voor het ontbreken van DMARC. Ondanks het feit dat de gedane pogingen tot cybercrime niet zijn geslaagd, zijn we gestart met de implementatie van DMARC. De implementatie is nagenoeg afgerond op het moment van dit schrijven – dus een dezer dagen is ook Arriva voorzien van deze veiligheidsmaatregel bovenop de al bestaande SPF en DKIM.

Arriva Nederland behoort overigens niet tot de vitale aanbieders zoals in de Wbni staan geformuleerd.
(…) Als je meer informatie wilt over dit specifieke besluit van het ministerie van IenW, dan kun je bij hen terecht.

Uit onderzoek van Zembla blijkt dat Arriva wel onder de wettelijke beschrijving van de vitale aanbieders in de Wbni valt, maar dat de spoorbedrijven door de minister nog niet expliciet heeft aangewezen als vitale aanbieder. Vergelijk de reactie van collega-spoorbedrijf DB Cargo:

Het proces waar de minister melding van maakt, is nog niet afgerond. Dat wil zeggen het aanwijzen van vitale aanbieders in de Nederlandse spoorsector heeft nog niet plaatsgevonden.

2. ASN Bank

Als de Volksbank, waar ASN Bank onderdeel van is, onderschrijven we het belang van veilige e-mailstandaarden zoals DMARC. DMARC kan onder andere helpen om phishing op eigen domeinen tegen te gaan. U heeft gelijk dat @asnbank.nl op het moment dat u dit testte nog niet optimaal beschermd was met DMARC en we lichten dit graag toe.

Zoals u vast al was opgevallen hebben wij als de Volksbank (toen nog SNS Bank N.V.) aan de genoemde factsheet van het NCSC een bijdrage geleverd, zijn we via de betaalvereniging lid van de veilige e-mail coalitie en schrijven collega's zelfs publiek artikelen die anderen helpen om minder vatbaar te worden voor phishing. DMARC is daar een onderdeel van.

Op basis daarvan zou u natuurlijk mogen verwachten dat we 'practise what you preach' toepassen, op al onze domeinen. Het is een continu proces om e-mail verkeer te optimaliseren.

Al langere tijd zijn nagenoeg al onze domeinen waar we niet mee mailen (zoals bijvoorbeeld @snsbank.nl [zie score op internet.nl]), gelijkende domeinen (zoals @www-asnbank.nl [zie score op internet.nl]) maar ook alle subdomeinen van onze merken (zoals @www.devolksbank.nl [score op internet.nl]) beschermd middels een DMARC (s)p=quarantaine of (s)p=reject. Dit om te voorkomen dat zodra onze hoofddomeinen optimaal zouden worden beschermd criminelen makkelijk zouden kunnen overstappen naar dat soort alternatieven.

Ook zijn alle e-mailstromen doorgelopen en hebben we soms zelfs bewust ervoor gezorgd dat niet alleen onze e-mailstroom werd verbeterd, maar ook die van andere klanten bij leveranciers. Een voorbeeld hiervan is de oproep van Spotler om in links echt eigen domeinnamen te gebruiken. Immers is ook de link in de e-mail een van de belangrijkste kenmerken om een echte e-mail van een valse te kunnen onderscheiden.

Waarom was de DMARC van @asnbank.nl dan op het moment van testen niet optimaal?

In onze architectuur hebben wij te maken met meerdere afhankelijkheden; zowel intern als extern. Voordat een aanpassing als DMARC goed doorgevoerd kan worden moesten alle partijen gebruikmaken van ons maildomein én voldoen aan DKIM of SPF zodat het DMARC beleid ook alleen

de slechte e-mail filtert. Door de grote volumes e-mail zou een niet volledig geoptimaliseerde configuratie zorgen voor onnodige uitval: een echte e-mail die toch in de spambox komt. Enkele afhankelijkheden waar wij als multi-merk bedrijf specifiek mee te maken kregen moesten ook worden opgelost. Denk bijvoorbeeld aan problematiek als een medewerker van een gedeelde afdeling (die een mailadres heeft @devolksbank.nl) ineens e-mail namens @asnbank.nl moest verzenden (waar DMARC niet mee kan omgaan). De voortgang van alle aanpassingen werd continue gemonitord, waarbij we ook eventuele gevallen van misbruik (bv. phishingsites) direct uit de lucht haalden. Om te voorkomen dat klanten legitieme e-mail in de spamfilter kregen, wat het geheel aan maatregelen ongedaan maakt, was bewust besloten om p=quarantaine pas in te stellen nadat als randvoorwaarde onze legitieme e-mail op orde was.

Er zijn dus de nodige stappen gezet waardoor we in de afgelopen periode ook DMARC hebben ingeschakeld. Indien u hertest zult u dan ook zien dat wij voor @asnbank.nl nu een p=reject hebben ingesteld.

En daarbij hanteren we ook een strike aanpak: onze SPF records bevatten een zeer beperkt aantal servers en waar leveranciers zijn toegevoegd zijn daarop strikte risico analyses toegepast.

Daar waar er een enkel domein nog niet optimaal beschermd is, wordt hier al aan gewerkt om dit wel het geval te maken.

Naast de bovenstaande antwoorden heeft u ook vragen gesteld over de aantallen cyberaanvallen. Cijfers hieromtrent worden gerapporteerd volgens de richtlijnen en indelingen zoals de ECB die voorschrijft en waarvoor toezichtsvertrouwelijkheid van toepassing is. Zodoende disclosen de toezichthouders noch de bank de informatie die betrekking heeft op vragen in deze categorie.

Afsluitend benadrukken we dat de Volksbank vanuit 'Veilig Bankieren' invulling aan haar plicht om te borgen dat bankieren veilig is voor onze klant en de bank. We dragen zorg voor een veilige afwikkeling van betalingen, serviceprocessen en bestrijden fraude en oplichting in het betalingsverkeer. Met waarborging van de (betaal)data. In dat kader zetten we ons actief in bij het verhogen van de cyberweerbaarheid van onze klanten, bijvoorbeeld met de zojuist gelanceerde training "Herken de Oplichter". En ook leveren we een actieve bijdrage aan goede samenwerking in de keten, zowel interbancair met andere private partijen als ook in de publiek-private samenwerking.

3. Centraal Orgaan Voorraadvorming Aardolieproducten

Kunt u aangeven waarom betreffende veiligheidsmaatregel (DMARC, DKIM, SPF) niet is genomen?

Sender Policy Framework, DKIM inbound en DMARC controle zijn reeds geruime tijd ingeregeld. Recent is ook uitgaande DKIM/DMARC ingeregeld.

Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?

Er zijn altijd pogingen, daarom worden Fortinet producten toegepast om aanvallen te detecteren en te blokkeren

Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.).

Malware, spear phising en dergelijke zijn zaken veel voorkomende vormen van Cybercrime.
Er worden tientallen mails geblokkeerd op dag basis door de secure e-mail filter. Hiervoor wordt de zwaarst mogelijke (full feature) Securemail tooling van Fortinet ingezet.

Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?

Er zijn geen succesvolle pogingen bekend.

Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?

Ja, COVA is in het kader van de Wbni aangewezen als aanbieder van een essentiële dienst (AED). In onze bedrijfsprocedures is ingeregeld dat incidenten bij ons en onze toeleveranciers onverwijld gemeld worden bij het NCSC.

Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?

Wij zijn door NCSC nooit actief benaderd over het ontbreken van specifiek benoemde veiligheidsissues. In algemene zin informeert het NCSC ons wel over dreigingen en succesvolle aanvallen elders.

Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?

Wij staan uiteraard altijd open voor suggesties ter verbetering van onze databeveiliging/e-mailverkeer.

4. Coteq

Coteq netbeheer verzorgt de distributie van gas en elektriciteit in een groot deel van Twente en de gemeente Hardenberg. Onze netten zijn onderdeel van de vitale energie-infrastructuur in het oosten van Nederland. Het veilig maken en houden van deze netten zit in het DNA van ons bedrijf. We doen er alles aan om te voorkomen dat energievoorziening voor onze klanten en onze bedrijfsvoering in gevaar komen. Wij voeren met regelmaat tests uit en monitoren het energienet 24/7u op eventuele bedreigingen. Onze medewerkers worden getraind om de organisatie weerbaar te houden tegen cybercriminaliteit.

Er bestaan vele vormen van cybercriminaliteit. Ook wij hebben last van pogingen tot deze criminaliteit. Ondanks genomen maatregelen hebben ook wij in de praktijk er wel eens mee te maken dat er op een verkeerde link wordt geklikt of dat er een besmet bestand wordt geopend. We beschikken over goed beveiligde systemen, goed opgeleide mensen en degelijke security-processen waardoor dergelijke acties niet tot verdere schade leiden of hebben geleid.

De implementatie van DMARC maakt deel uit van de maatregelen die wij nog gaan treffen. DMARC is naast SPF en DKIM een extra beveiligingsmaatregel dat meehelpt in het voorkomen dat anderen digitale identiteitsfraude kunnen plegen en zich kunnen voordoen als medewerkers van Coteq. Digitale identiteitsfraude is slechts één facet van cybercriminaliteit, waarbij DMARC een extra laag bescherming geeft. Voor de overige vormen van cybercriminaliteit zijn andere gepaste maatregelen ingezet. We blijven ons continue inzetten met een breed en gelaagd scala aan maatregelen om alle vormen van cybercriminaliteit nu en in de toekomst tegen te gaan.

5. DB Cargo Nederland

Deutsche Bahn is continuously working on IT security. However, no one can guarantee 100 percent security. The DMARC specification is an additional security measure for e-mails - in addition to many other security measures that are always kept up to date at DB. In this context, DMARC is also already activated in a reporting mode, is continuously evaluated to then ensure a smooth realization of the block mode.

(…)

Het proces waar de minister melding van maakt, is nog niet afgerond. Dat wil zeggen het aanwijzen van vitale aanbieders in de Nederlandse spoorsector heeft nog niet plaatsgevonden.

6. Dunea

Drinkwaterbedrijven vinden het belangrijk om veilige diensten te leveren. Ondanks alle zorg en inzet hiervoor, kúnnen er kwetsbaarheden in de beveiliging zitten (of een vermoeden daartoe). Meldingen van eventuele kwetsbaarheden helpen ons om te kijken waar verbeteringen mogelijk zijn. De sector voert dan ook sinds 2014 een zogenoemd coördinated vulnerability disclosure (CVD) beleid, gebaseerd op de Leidraad van het NCSC. Dat geldt ook voor Dunea.

Op onze website (www.dunea.nl/beveiliging) stimuleren wij het melden van eventuele kwetsbaarheden door externe partijen, zoals Stichting Internet Cleanup Foundation, volgens de daartoe opgestelde richtlijnen. Wij nemen in dat geval de melding in behandeling en nemen binnen een aantal werkdagen contact op met de melder om afspraken te maken over een redelijke herstelperiode (indien dat van toepassing is) en een eventuele gecoördineerde publicatie van het beveiligingslek.

Naar aanleiding van de veiligheidscheck die u hebt gedaan, hebt u een aantal concrete vragen gesteld aan Dunea. Deze vragen beantwoorden wij hieronder.

1. Kunt u aangeven waarom betreffende veiligheidsmaatregel (strikte DMARC policy) niet is genomen?

Het NCSC geeft adviezen en handelingsperspectief aan vitale bedrijven, waaronder de tien Nederlandse drinkwaterbedrijven, over kwetsbaarheden en dreigingen. Als drinkwaterbedrijf acteren wij weloverwogen en proactief, op gedegen eigen risicoanalyses, wettelijke eisen en adviezen van het NCSC.

Voor het beschermen van domeinnamen tegen e-mailfraude zijn verschillende maatregelen mogelijk. DMARC is één van die maatregelen. Wij hebben diverse maatregelen getroffen, waaronder implementatie van DMARC. Het strikter instellen van DMARC staat op de planning, als onderdeel van het voortdurend bijstellen van ons totale pakket aan maatregelen tegen cybercrime.

2. Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?

Wij maken onderscheid tussen procesautomatisering en kantoorautomatisering. In het meest recente Cyber Security Beeld Nederland (CSBN) staat dat gerichte aanvallen op de vitale processen (procesautomatisering) in Nederland niet zijn waargenomen.

Het onderzoek van Zembla/Stichting Internet Cleanup Foundation richt zich op de mailserver. Die is onderdeel van de kantoorautomatisering en staat los van de vitale processen. Zoals te lezen is in het CSBN van de afgelopen jaren, worden drinkwaterbedrijven o.a. geconfronteerd met ransomware- en phishingaanvallen in de kantoorautomatiseringsomgeving. Dat geldt ook voor Dunea. Wij voeren actief beleid om ons daar tegen te wapenen.

3. Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)

Vanuit beveiligingsoptiek is specifieke informatie over pogingen tot cybercriminaliteit vertrouwelijk.

4. Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?

Vanuit beveiligingsoptiek is specifieke informatie over pogingen tot cybercriminaliteit vertrouwelijk.

5. Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?

Ja, de tien Nederlandse drinkwaterbedrijven zijn benoemd tot aanbieders van essentiële diensten (AED's) en vallen derhalve onder de Wbni. Op basis van de Wbni hebben drinkwaterbedrijven een meldplicht bij het NCSC en de sectorale toezichthouder, de ILT.

De wettelijke meldplicht op basis van de Wbni betreft incidenten en/of inbreuken die aanzienlijke gevolgen (kunnen) hebben voor de continuïteit van de vitale dienst. Bij drinkwaterbedrijven gaat het hierbij om de drinkwatervoorziening. Bij Dunea hebben zich geen incidenten voorgedaan die onder deze meldplicht vallen.

E-mail-fraude gerelateerd aan kantoorautomatisering, zoals bedoeld in het onderzoek van Zembla en Stichting Internet Cleanup Foundation, staat los van de continuïteit van de drinkwatervoorziening. Een eventueel incident op dit gebied is dan ook niet meldplichting.

6. Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?

Het NCSC heeft in 2015 een factsheet gepubliceerd over bescherming van domeinnamen tegen phishing. Zoals bij vraag 1 staat uiteengezet, nemen wij op basis van mogelijke risico's maatregelen en maken wij een afweging om al dan niet aanvullende maatregelen te treffen. Als drinkwaterbedrijf zijn wij immers zelf verantwoordelijk voor bescherming van beschikbaarheid, integriteit en vertrouwelijkheid van onze data en systemen én het managen van eventuele risico's rondom deze data en systemen.

Dunea is niet individueel door het NCSC gewaarschuwd vanwege het ontbreken van een strikte DMARC-policy in onze mailserver.

7. Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?

Maatregelen om de weerbaarheid tegen cybercrime te vergroten zijn als volgt te categoriseren:

1. *Reductie van bedreiging*
2. *Preventie, detectie en repressie van incidenten*
3. *Correctie in het geval dat zich toch incidenten voordoen*

Wij investeren in alle genoemde typen maatregelen tegen cybercrime.

Meldingen van eventuele kwetsbaarheden in de beveiliging van onze diensten nemen wij altijd serieus. Dat geldt ook voor het onderzoek van Zembla en Stichting Internet Cleanup Foundation. Wij zullen de bevindingen van het onderzoek evalueren en bezien of aanvullende en/of andersoortige maatregelen noodzakelijk zijn.

Een aanscherping van onze DMARC policy staat bij ons op de planning. Dit is onderdeel van het voortdurend bijstellen van ons totale pakket aan maatregelen tegen cybercrime. Wij onderzoeken momenteel of deze aanscherping versneld moet worden doorgevoerd.

7. Enduris

Stedin en Enduris/DNWG zijn netbeheerders van het gas- en elektriciteitsnet in Zuid-Holland, Utrecht en Zeeland. Deze netten zijn onderdeel van de vitale energie-infrastructuur van het meest stedelijke gebied van Nederland. Het veilig maken en houden van deze netten zit in het DNA van ons bedrijf. We spannen ons optimaal in om onze systemen in stand te houden. We doen er alles aan om te voorkomen dat energievoorziening voor onze klanten en onze bedrijfsvoering in gevaar komen. Wij voeren regelmatig tests uit en monitoren het energienet 24/7u op eventuele bedreigingen en onze

ruim 5000 medewerkers worden actief getraind om de organisatie weerbaarder te maken tegen cybercriminaliteit.

Er bestaan vele vormen van cybercriminaliteit. Ook wij hebben last van pogingen tot deze criminaliteit. Ondanks genomen maatregelen hebben ook wij in de praktijk er wel eens te maken dat er op een verkeerde link wordt geklikt of een besmet bestand wordt geopend. We beschikken over goed beveiligde systemen waardoor dergelijke acties in de kiem gesmoord worden en niet tot verdere schade leiden of hebben geleid.

We zijn op dit moment bezig met de implementatie van DMARC. DMARC is naast SPF en DKIM een extra beveiligingsmaatregel dat meehelpt in het voorkomen dat anderen digitale identiteitsfraude kunnen plegen en zich kunnen voordoen als medewerkers van Stedin of Enduris/DNWG. Digitale identiteitsfraude is slechts één facet van cybercriminaliteit, waarbij DMARC een extra laag bescherming geeft. Voor de overige vormen van cybercriminaliteit zijn andere gepaste maatregelen ingezet. We blijven ons continue inzetten met een breed en gelaagd scala aan maatregelen om alle vormen van cybercriminaliteit nu en in de toekomst tegen te gaan.

8. Enexis

Enexis Netbeheer is een regionale netbeheerder. Wij zorgen ervoor dat miljoenen klanten in de provincies Groningen, Drenthe, Overijssel, Noord-Brabant en Limburg elektriciteit en gas kunnen ontvangen en terugleveren. Van alle kanten stroomt energie ons netwerk binnen. Enerzijds via grootschalige energieproducenten, anderzijds via klanten die energie duurzaam opwekken en aan ons (terug)leveren. We hebben een prominente rol in de keten van energie en zetten ons in voor verduurzaming van het energiesysteem in Nederland.

Wij zijn ons terdege bewust van onze rol in de vitale infrastructuur van ons land. Door een toenemend belang van ICT en cybersecurity is digitale veiligheid één van onze speerpunten. We nemen continu structurele maatregelen om onze ICT infrastructuur en energienetwerken te beschermen. In onze aanpak van digitale veiligheid focussen we niet alleen op technologie, maar ook op mensen, processen en cultuur en zijn wij een lerende organisatie. Zo testen wij regelmatig en proactief het beveiligingsniveau van onze systemen, monitoren onze systemen 24/7 en trainen onze medewerkers actief op het herkennen én voorkomen van cyberdreigingen.

De complexiteit van digitale veiligheid groeit. Dit vraagt van ons continue alertheid. We zoeken hierbij doorlopend het optimum om Enexis Groep te beschermen tegen cybersecurity-aanvallen. Processen moeten echter ook werkbaar blijven en maatschappelijk geld willen wij zorgvuldig investeren.

Om ons bedrijf zo veilig mogelijk te houden, hebben we intensief contact met o.a. het Nationaal Cyber Security Center, toezichthouders en sectorgenoten over potentiële risico's en bedreigingen. Onze eigen cybersecurityspecialisten maken onderdeel uit van meerdere kennisnetwerken bij bedrijven in de energiesector en binnen de overheid. Op deze wijze delen we snel waardevolle kennis over incidenten, dreigingen en kwetsbaarheden. Zodoende zijn we snel en adequaat in staat maatregelen te nemen om cybercriminelen en andere kwaadwillenden buiten de deur te houden en schade te voorkomen.

Meldingen over cybersecurity, knelpunten en kwetsbaarheden behandelen wij binnen Enexis Groep met de hoogste prioriteit. Wij waarderen uw bericht dan ook enorm. Het is echter ook ons beleid om informatie over onze beveiligingsmaatregelen en die van onze (keten)partners in principe niet te delen of slechts op hoofdlijnen te delen met externe partijen.

Wij zijn momenteel bezig met de verdere/striktere implementatie van DMARC. Daarbij merken wij op dat beveiligingstandaarden zoals DKIM, SPF en DMARC zich vooral richten op de beveiliging van digitale identiteiten en op deze wijze identiteitsfraude moet voorkomen. Belangrijk is te weten dat onze vitale netwerken ontkoppeld zijn van de ICT-infrastructuur van Enexis Groep en dat wij in onze

emailsystemen belangrijke beveiligingsmaatregelen hebben geïmplementeerd, zoals geavanceerde realtime monitoring van cyberdreigingen.

Wij danken u voor het onderzoek en de specifieke melding, zodat wij en andere organisaties hiervan kunnen leren.

9. Engie

Helaas kan ik de vragen niet beantwoorden. ENGIE heeft als beleid om niet inhoudelijk te reageren op vragen mbt cybersecurity.

10. EPZ (exploitant kerncentrale Borssele)

Wij danken de redactie van Zembla voor de melding. EPZ neemt iedere melding over de veiligheid en beveiliging van ons bedrijf serieus. Iedere melding wordt inhoudelijk bekeken en (zo nodig) opgevolgd met maatregelen.

Als het gaat om de beveiliging (security) van ons bedrijf, doen wij naar buiten toe meestal geen inhoudelijke mededelingen. In uw geval willen we daar (tot op zekere hoogte) een uitzondering op maken. Dit vanwege uw rol en onze eigen verantwoordelijkheid in het maatschappelijk debat. Wij beseffen dat er mogelijk onrustgevoelens kunnen ontstaan als er vragen blijven hangen over onze (cyber)security. Wel vragen wij uw begrip voor het feit dat wij niet in detail zullen treden.

De door u uitgevoerde screening ziet niet alle aanwezige securitymaatregelen. Die zijn robuuster dan uit uw screening blijkt. Zonder al te veel in detail te gaan: het berichtenverkeer van en naar EPZ is niet direct aan internet gekoppeld. Bovendien vindt in deze losgekoppelde omgeving controle plaats op de betrouwbaarheid van mailberichten.

Kort samengevat: EPZ beschikt over een door de overheid goedgekeurd beveiligingspakket. Daarin ligt ook een meldingsplicht vast voor incidenten met (middel) grote impact. Net als iedere andere Nederlander of Nederlandse organisatie staan wij bloot aan de door u geschetste criminele methodes. Wij zijn geen uitzondering. Omdat wij goed weerstand kunnen bieden aan cybercriminaliteit en dit permanent monitoren, kunnen wij stellen dat geen enkele poging succesvol was. Er waren dus wel pogingen, maar die leidden niet tot incidenten. Er was geen schade en er hoefde ook geen melding te worden gedaan bij de toezichthouders.

Ten aanzien van uw vragen over de DMARC-policy kunnen wij u mededelen dat wij alert zijn op verbeteringen. Dit geldt voor alles wat onze veiligheid en beveiliging betreft. De DMARC-aanscherping is bij onze organisatie reeds in behandeling. Afgelopen zomer is een deel van de adviezen al overgenomen. Voor een aantal aspecten geldt dat eerst de meerwaarde voor onze organisatie wordt beoordeeld. Deze maand volgt de afronding van de implementatie van de striktere policy.

Tot slot: wij doen geen mededelingen over het doen en laten van andere organisaties. Echter, u kunt er op vertrouwen dat als wij een (cyber)security melding ontvangen van NCSC (of in uw geval van ZEMBLA) wij die serieus nemen. Als dat nodig is, volgt er actie.

Wij hopen u hiermee afdoende van informatie te hebben voorzien, meer details zullen wij u om voor de hand liggende redenen niet verstrekken.

Na vervolgvragen laat EPZ weten:

Alle NCSC veiligheidsmeldingen komen bij EPZ terecht bij de IT security betrokken personen. Vervolgens wordt beoordeeld of ze van toepassing zijn op onze ICT-inrichting: het nut en de noodzaak. Indien dat het geval is dan wordt de aanbeveling aansluitend doorgevoerd. De snelheid van doorvoeren is afhankelijk van de combinatie "kans (dat een kwetsbaarheid benut wordt) x effect (dat hierdoor kan worden veroorzaakt)".

EPZ heeft de beveiliging van het emailverkeer op een andere wijze beveiligd.

De implementatie van DMARC is slechts voor mail naar buiten om de echtheid van onze mails te kunnen valideren.

Dat neemt niet weg dat we van toepassing zijnde aanbevelingen hebben overgenomen.

EPZ heeft te maken gehad met pogingen van ransomware. Zoals aangegeven in onze eerste reactie staat EPZ bloot aan de door u geschetste criminele methodes; ook ransomware. Wij zijn geen uitzondering. Omdat wij goed weerstand kunnen bieden aan cybercriminaliteit en dit permanent monitoren, kunnen wij stellen dat geen enkele poging succesvol was. Er waren dus wel pogingen, maar die leidden niet tot incidenten.

Op uw vraag over de nucleaire veiligheid als hackers onverhoopt zou lukken de centrale binnen te komen, het volgende.

De vragen die Zembla ons tot op heden gesteld heeft, beperkten zich tot de security van ons mailverkeer. In deze nieuwe vraag legt u een verband tussen mailverkeer en de nucleaire veiligheid. Wij kunnen daar wel wat dieper op ingaan. Het reactorbeveiligingssysteem van de kerncentrale is analoog. Dit kan dus per definitie niet gehackt worden. In de kerncentrale is geen enkel vitaal bedieningssysteem aangesloten op het internet. De procesinstallaties zijn van buitenaf dus niet benaderbaar. Het aansturen van het nucleaire proces en de bediening van de reactor gebeurt met analoge techniek, welke ongevoelig is voor digitale verstoringen. Verstoring van ICT-systemen rond de kerncentrale heeft daarom geen invloed op de beschikbaarheid van de bedieningsinstrumenten. Deze staan immers helemaal los van ICT-aansturing. De overige in onze kerncentrale aanwezige ICT-systemen zijn slechts ondersteunend en worden bovendien streng beveiligd.

11. Essent

1. Kunt u aangeven waarom betreffende veiligheidsmaatregel (DKIM + strikte DMARC-policy) niet is genomen?

Antwoord: Essent maakt gebruik van DKIM voor alle email die klanten van ons ontvangen. En met de implementatie van DMARC zijn we heel ver. De verwachting is dat we heel snel ook hierin de allerlaatste stap kunnen zetten zodat we helemaal DMARC-proof zijn. Deze laatste stap houdt in dat valse emails niet alleen worden geïdentificeerd zoals nu al het geval is, maar ook worden geblokkeerd.

2. Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?

Antwoord: iedere organisatie wordt vandaag de dag geconfronteerd met cybercriminaliteit. Over de details kunnen wij helaas geen uitspraken doen. Het spreekt voor zich dat als er sprake is van een aanval, wij hiervoor de gebruikelijke processen in gang zetten en instanties en toezichthouders hierover informeren.

3. Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)

Zie 2.

4. Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?

Zie 2.

5. Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?

Antwoord: Essent wordt door het Wbni niet aangemerkt als vitaal. Vitale bedrijven binnen de energiesector zijn die bedrijven die ook daadwerkelijk energie transporteren en distribueren. Essent hoort daar niet bij. Dit betekent dat wij niet gebonden zijn aan het normenkader wat door de NCSC wordt gehanteerd, inclusief de specifieke DMARC-eisen. Echter heeft Essent de veiligheid van haar klanten hoog in het vaandel en gelooft ook in de technische veiligheidsmaatregelen zoals de DMARC-Policy, vandaar dat wij deze policy dan ook implementeren (zie ook ons antwoord op vraag 1). En hanteren wij net zoals onze moeder E.ON, de internationale ISO veiligheidsnorm 27001 voor informatiebeveiliging.

(De woordvoerder van Essent geeft later telefonisch aan wel tot de vitale sector te behoren, maar sinds de overname door E.ON in 2020 geen vitale aanbieder meer te zijn, omdat het (moeder)bedrijf zelf geen energie meer produceert.)

6. Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?

Antwoord: omdat Essent niet wordt aangemerkt als vitale organisatie worden wij tot op heden niet actief door het NCSC benaderd.

7. Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?

Antwoord: zoals ook bij vraag 1 en 5 aangegeven hanteert Essent een proactief risicobeleid en vinden wij het ondanks dat wij hiertoe niet verplicht zijn gesteld, belangrijk onze DMARC implementatie aan te vullen met een DMARC-policy. Wij verwachten heel snel ook de laatste stap hierin te kunnen zetten zodat klanten nog beter worden beschermd tegen valse emails.

Later mailt Essent:

Als aanvulling op de eerdere reactie van mijn collega wil ik u graag informeren dat wij half september ook de laatste stap hebben gezet en DMARC inmiddels succesvol is geïmplementeerd.

12. Euronext

Een team van cyberspecialisten binnen Euronext monitort, analyseert en werkt op continue basis aan de mitigatie van cyberdreigingen voor onze systemen. Digitale identiteitsfraude valt hier ook onder. Om veiligheidsredenen communiceren we niet met externe partijen over mogelijke dan wel het aantal cyberdreigingen dat door onze teams wordt geïdentificeerd, noch over de exacte maatregelen die we nemen met betrekking tot cybersecurity. We kunnen wel bevestigen dat dreigingen altijd onmiddellijk worden gemeld aan de relevante autoriteiten.

Het NCSN informeert en adviseert bedrijven, waaronder Euronext, over digitale dreigingen en mogelijke kwetsbaarheden. Zij hebben een aantal basismaatregelen geformuleerd, onder meer voor het gebruik van moderne internetstandaarden. Met betrekking tot digitale identiteitsfraude biedt DMARC extra bescherming. Dit is reeds geïmplementeerd binnen Euronext, en wordt verder versterkt, zoals het onderzoek aangeeft.

In zijn algemeenheid geldt dat het beschikbaar houden van alle systemen, diensten en informatie voor onze bedrijfsvoering en voor onze klanten een prioriteit is voor Euronext. Dit betekent het waarborgen dat onze informatiesystemen betrouwbaar en volledig zijn, en niet verstoord worden. Het is van belang te waarborgen dat deze informatiesystemen enkel toegankelijk zijn voor mensen of door systemen waaraan toestemming is verleend. Wij verbeteren onze systemen om die reden continue, en zullen dit blijven doen.

13. Evides

Drinkwaterbedrijven vinden het belangrijk om veilige diensten te leveren. Ondanks alle zorg en inzet hiervoor, kúnnen er kwetsbaarheden in de beveiliging zitten (of een vermoeden daartoe).

Op de websites van drinkwaterbedrijven wordt het melden van eventuele kwetsbaarheden door externe partijen, zoals The Internet Cleanup Foundation, aangemoedigd via de hiervoor bedoelde processen. Tegelijkertijd hebben we een intern bewustwordingsprogramma cybersecurity. Meldingen van eventuele kwetsbaarheden helpen ons om te kijken waar verbeteringen mogelijk zijn. De sector voert dan ook sinds 2014 een zogenoemd Coördinated Vulnerability Disclosure (CVD) beleid (gebaseerd op de Leidraad van het NCSC) . Bedrijven nemen de melding in behandeling en nemen binnen een aantal werkdagen contact op met de melder om afspraken te maken over een redelijke herstelperiode (indien dat van toepassing is) en een eventuele gecoördineerde publicatie van het beveiligingslek.

Voor Evides Waterbedrijf geldt dat cyber security een zeer hoge prioriteit heeft. Het onderwerp heeft en krijgt continue aandacht binnen het bedrijf.

Vragen

1. Kunt u aangeven waarom betreffende veiligheidsmaatregel (DMARC) niet is genomen?

Het NCSC geeft adviezen en handelingsperspectief aan vitale bedrijven, waaronder de tien Nederlandse drinkwaterbedrijven, over kwetsbaarheden en dreigingen. Als drinkwatersector acteren wij weloverwogen en proactief op gedegen eigen risicoanalyses, wettelijke eisen en adviezen van het NCSC.

Optioneel: Voor het beschermen van domeinnamen tegen e-mailfraude zijn verschillende maatregelen mogelijk.

2. Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?

In het Cyber Security Beeld Nederland (CSBN) is te lezen dat drinkwaterbedrijven o.a. worden geconfronteerd met pogingen tot ransomware- en phishingaanvallen in de kantoorautomatiseringsomgeving. Wij voeren actief beleid om ons daar tegen te wapenen.

Ook staat in het Cyber Security Beeld Nederland (CSBN) dat gerichte aanvallen op de vitale processen (waaronder de drinkwatervoorziening) in Nederland niet zijn waargenomen.

3. Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)

Zie vraag 2.

4. Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?

Vanuit beveiligingsoptiek is specifieke informatie over pogingen tot cybercriminaliteit vertrouwelijk.

5. Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?

Ja, de tien Nederlandse drinkwaterbedrijven zijn aangewezen tot aanbieders van essentiële diensten (AED's) en vallen derhalve onder de Wbni. Op basis van de Wbni hebben drinkwaterbedrijven een meldplicht bij het NCSC en de sectorale toezichthouder, de ILT.

De wettelijke meldplicht op basis van de Wbni betreft incidenten en/of inbreuken die aanzienlijke gevolgen (kunnen hebben) voor de continuïteit van de vitale dienst. Bij drinkwaterbedrijven gaat het hierbij om de drinkwatervoorziening. De melding van The Internet Cleanup Foundation heeft daar geen betrekking op.

6. Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?

Het NCSC heeft in 2015 een factsheet gepubliceerd over bescherming van domeinnamen tegen phishing. Zoals bij vraag 1 staat uiteengezet, nemen drinkwaterbedrijven op basis van mogelijke risico's maatregelen en maken een afweging om al dan niet aanvullende maatregelen te treffen. Drinkwaterbedrijven zijn immers zelf verantwoordelijk voor bescherming van beschikbaarheid, integriteit en vertrouwelijkheid van hun data en systemen én het managen van evt. risico's rondom deze data en systemen.

7. Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?

Meldingen van eventuele kwetsbaarheden in de beveiliging van onze diensten nemen wij altijd serieus. Dat geldt ook voor het onderzoek van The Internet Cleanup Foundation. Wij zullen de bevindingen van het onderzoek evalueren en bezien of aanvullende en/of andersoortige maatregelen noodzakelijk zijn.

In een latere reactie meldt Evides:

In aanvulling op onze eerdere reactie melden wij u dat we inmiddels de veiligheidsmaatregelen op onze systemen hebben aangescherpt, waardoor wij voldoen de DMARC policy.

14. KLM

Betrouwbaarheid en veiligheid zijn topprioriteiten voor KLM.

Daarbij hoort ook de voortdurende bescherming van passagiers, klanten, leveranciers en de eigen KLM-organisatie tegen pogingen tot binnendringen en misleidende communicatie van kwaadwillenden.

KLM monitort veiligheidsrisico's continu en probeert bijvoorbeeld cyberaanvallen, (spear)phishing , CEO fraude, spoofing en malware, gericht tegen, of uit naam van KLM, te voorkomen, op te sporen en, waar mogelijk, direct te mitigeren.

Als onderdeel hiervan is KLM enkele jaren geleden al gestart met de implementatie van de nieuwe technologie: SPF, DKIM en DMARC. De implementatie van SPF en DKIM is ondertussen volledig afgerond. De implementatie van DMARC verkeert op dit moment in de afrondende fase. KLM benadrukt dat de implementatie van DMARC geen enkel effect heeft op onze vliegoperatie.

KLM is een vitale aanbieder en valt onder de meld- en zorgplicht van de Wbni. KLM onderhoudt hiervoor goed contact met het NCSC en andere delen van de Nederlandse overheid. Mocht daarvoor aanleiding zijn, dan zal er door KLM altijd melding worden gemaakt.

Voor jouw eigen achtergrond: ons beleid is dat we eigenlijk geen uitspraken doen over specifieke security-onderwerpen, in de breedste zin van het woord. We hebben gepoogd antwoord te geven waar mogelijk binnen dit beleid.

15. Luchtverkeersleiding Nederland

1. Kunt u aangeven waarom betreffende veiligheidsmaatregel (DMARC) niet is genomen?

Cyber security is een van de topprioriteiten van LVNL. Als aanbieder van vitale infrastructuur hechten we grote waarde aan onze cyber weerbaarheid. LVNL heeft hiervoor een security roadmap waarin mede beveiligingsmaatregelen voor het e-mail verkeer zijn opgenomen. De genoemde maatregelen SPF en DKIM zijn al ingevoerd. DMARC staat ook op de security roadmap en wordt op korte termijn ingevoerd. Hiervoor was eerst een aanpassing nodig in een ander systeem omdat deze niet compatibel was met DMARC. Met dit systeem dienen onder meer sportvliegers hun vliegplan in. Het aanbieden van deze dienst is een wettelijk taak van LVNL. In samenspraak met partners die betrokken zijn bij onze cyberbeveiliging is besloten eerst de noodzakelijke technische aanpassing in dit systeem door te voeren. Nu dit is afgerond is ook de invoering van DMARC opnieuw in gang gezet.

2. Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?

3. Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)

Er is sprake geweest van pogingen tot cybercrime. Alle pogingen zijn succesvol afgeslagen. Over welke vormen van cybercrime dit waren doen we vanuit veiligheidsoogpunt geen mededelingen.

4. Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?

Nee, deze waren niet succesvol. Door onze cybersecurity maatregelen heeft geen enkele poging geleid tot een veiligheidsissue met materiële of immateriële schade als gevolg.

5. Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?

LVNL is, als onderdeel van de aanbieders van vitale infrastructuur, aangewezen als aanbieder van zogenoemde essentiële diensten. Wbni kent een meldplicht en een zorgplicht. Dat betekent dat alle incidenten door LVNL worden gemeld aan de NCSC.

6. Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?

LVNL wordt regelmatig benaderd door het NCSC betreffende cyberdreigingen en kwetsbaarheden. Wij doen geen mededelingen over de inhoud hiervan.

7. Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?

DMARC staat in de security roadmap en wordt zoals eerder aangegeven doorgevoerd.

16. Nederlandse Aardolie Maatschappij

1. *Kunt u aangeven waarom betreffende veiligheidsmaatregel (DMARC met strikte policy) niet is genomen?*

Deze instelling was een bewuste keuze, strikter zetten had mogelijk gevolg voor e-mail communicatie met derden.

2. *Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?*

Bij veel grotere bedrijven is cybercrime een thema, dat is zelfs op dit moment ook voor veel particulieren al het geval. Wij gaan niet in op cybercrime gerelateerde zaken met betrekking tot NAM

3. *Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)*

Hackers proberen verschillende manieren uit om bedrijven te hacken.

4. *Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?*

Ik verwijs naar antwoord op vraag 2

5. *Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?*

Ik verwijs naar antwoord op vraag 2

6. *Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?*

Ik verwijs naar antwoord op vraag 2

7. *Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?*

Ik verwijs naar antwoord op vraag 1

17. PWN / Drinkwater Noord Holland

Drinkwaterbedrijven vinden het belangrijk om veilige diensten te leveren. Ondanks alle zorg en inzet hiervoor, kúnnen er kwetsbaarheden in de beveiliging zitten (of een vermoeden daartoe).

Op de websites van drinkwaterbedrijven wordt het melden van eventuele kwetsbaarheden door externe partijen, zoals The Internet Cleanup Foundation, aangemoedigd via de hiervoor bedoelde processen. Meldingen van eventuele kwetsbaarheden helpen ons om te kijken waar verbeteringen mogelijk zijn. De sector voert dan ook sinds 2014 een zogenoemd Coördinated Vulnerability Disclosure (CVD) beleid (gebaseerd op de Leidraad van het NCSC) . Bedrijven nemen de melding in behandeling en nemen binnen een aantal werkdagen contact op met de melder om afspraken te maken over een redelijke herstelperiode (indien dat van toepassing is) en een eventuele gecoördineerde publicatie van het beveiligingslek.

Vragen

1. *Kunt u aangeven waarom betreffende veiligheidsmaatregel (DMARC) niet is genomen?*

PWN is continu bezig met het verbeteren van haar informatiebeveiliging. PWN prioriteert verbeteracties op basis van gedegen Risicoanalyses, wettelijke eisen en adviezen van het NCSC. Deze maatregel had PWN al in het vizier, er lopen en verwachten de implementatie van DMARC binnenkort te voltooien.

2. *Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?*

Alle organisaties wereldwijd die gebruik maken van het internet zijn dagelijks doelwit van pogingen tot cybercrime. Zoals te lezen is in het Cyber Security Beeld Nederland (CSBN) van de afgelopen jaren, worden drinkwaterbedrijven onder andere geconfronteerd met phishingaanvallen en pogingen tot ransomwarebesmettingen in de kantoorautomatiseringsomgeving. Ook PWN heeft te maken met pogingen tot cybercrime. In het meest recente CSBN staat dat drinkwaterbedrijven onder andere worden geconfronteerd met pogingen tot ransomware- en phishingaanvallen in de kantoorautomatiseringsomgeving. Wij voeren actief beleid om ons daar tegen te wapenen. Ook staat in het CSBN dat gerichte aanvallen op de vitale processen (waaronder de drinkwatervoorziening) in Nederland niet zijn waargenomen.

3. Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)

Zie vraag 2.

4. Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?

Vanuit beveiligingsoptiek is specifieke informatie over pogingen tot cybercriminaliteit vertrouwelijk.

5. Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?

Ja, de tien Nederlandse drinkwaterbedrijven zijn benoemd tot aanbieders van essentiële diensten (AED's) en vallen derhalve onder de Wbni. Op basis van de Wbni hebben drinkwaterbedrijven een meldplicht bij het NCSC en de sectorale toezichthouder, de ILT.

De wettelijke meldplicht op basis van de Wbni betreft incidenten en/of inbreuken die aanzienlijke gevolgen (kunnen hebben) voor de continuïteit van de vitale dienst. Bij drinkwaterbedrijven gaat het hierbij om de drinkwatervoorziening. De melding van The Internet Cleanup Foundation heeft daar geen betrekking op.

6. Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?

Het NCSC heeft in 2015 een factsheet gepubliceerd over bescherming van domeinnamen tegen phishing. Zoals bij vraag 1 staat uiteengezet, nemen drinkwaterbedrijven op basis van mogelijke risico's maatregelen en maken een afweging om al dan niet (aanvullende) maatregelen te treffen. Drinkwaterbedrijven zijn immers zelf verantwoordelijk voor bescherming van beschikbaarheid, integriteit en vertrouwelijkheid van hun data en systemen én het beheersen van eventuele risico's rondom deze data en systemen.

7. Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?

Meldingen van eventuele kwetsbaarheden in de beveiliging van onze diensten nemen wij altijd serieus. Aan de hand van het onderzoek van The Internet Cleanup Foundation zullen wij de getroffen maatregelen opnieuw evalueren.

18. Reactor Instituut Delft

Lieten telefonisch weten geen antwoorden te geven op vragen over cyberveiligheid.

19. RWE

Waarom zijn deze veiligheidsmaatregelen (DMARC) niet genomen?

Als een van de grootste elektriciteitsproducenten in Europa levert RWE een belangrijke bijdrage aan de continuïteit van de voorziening. Om dit te kunnen garanderen, moeten wij onze infrastructuur goed beveiligen. Daarom zijn onze IT-beveiligingsspecialisten voortdurend bezig met het optimaliseren van de beveiligde infrastructuur bij RWE. In dit verband hebben wij onlangs verdere veiligheidsmaatregelen vastgesteld. DMARC behoort tot deze maatregelen en zal op korte termijn operationeel zijn. Tot nu toe zijn de bijbehorende risico's beperkt gebleven door aanvullende voorzorgsmaatregelen.

Zijn er in uw organisatie in de afgelopen 5 jaar (pogingen tot) cybercriminaliteit geweest? Zo ja, om welk type cybercriminaliteit ging het (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, gegevensdiefstal, ddos-aanvallen, ransomware, etc.)?

Zoals elk groot bedrijf merken ook wij een groot aantal pogingen van het hierboven genoemde soort. Daarom hebben wij bij RWE uitgebreide maatregelen genomen om onze goed beveiligde infrastructuur voortdurend te controleren en te verbeteren. Naast technische voorzorgsmaatregelen omvat dit ook het opleiden van onze medewerkers en hun bewustwording van informatiebeveiliging.

Zo ja, in welke mate waren deze pogingen succesvol? Hoe groot was de materiële en immateriële schade?

Wij hebben in de genoemde periode geen noemenswaardige schade ondervonden.

Behoort uw organisatie tot de belangrijke aanbieders zoals geformuleerd in de Wbni? Zo ja, is er een incident gemeld bij het NCSC?

Het IT-systeem van RWE en het communicatiesysteem voor de technische installaties (het zogenaamde OT-gebied) van RWE lopen om veiligheidsredenen gescheiden van elkaar. Sinds 1 juni 2021 wordt het OT-systeem van RWE beschouwd als een essentiële dienstverlener in de zin van de WBNI, waarvoor bijzonder hoge cybersecurity-eisen gelden. Tot op heden hebben zich op dit gebied geen beveiligingsrelevante gevallen voorgedaan die aan het Nederlandse Nationaal Cyber Security Centrum (NCSC) moesten worden gemeld.

Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze beveiligingsmaatregel(en) in uw mailserver?

RWE werkt nauw samen met de nationale instanties die verantwoordelijk zijn voor de informatiebeveiliging op haar locaties. Wij zijn niet op de hoogte van gevallen waarin het NCSC een waarschuwing heeft gegeven voor het niet beveiligen van onze mailservers.

Bent u van plan maatregelen te nemen als gevolg van de onderzoeksbevindingen? Zo ja, welke? Zo nee, waarom niet?

Ongeacht de resultaten van dit onderzoek hebben wij maatregelen gepland, zoals de implementatie van DMARC. Deze zullen op korte termijn worden geïmplementeerd.

20. Schiphol

Cyber security is één van Schiphol's topprioriteiten. Schiphol investeert continu met een breed scala aan maatregelen in het veilig houden van IT-systemen op de luchthaven. Bijvoorbeeld door te werken met een cyber security roadmap om veiligheidsmaatregelen helder te kunnen prioriteren en

implementeren om zo in te spelen op daar waar de dreiging het grootst is. We geven hierover ook jaarlijks inzage in ons jaarverslag.

Schiphol heeft verschillende veiligheidsmaatregelen geïmplementeerd, zoals SPF, DKIM en DMARC. Het is ons bekend dat de strikte DMARC Quarantine/Reject policy niet is geactiveerd. De mogelijkheden voor het activeren van een strikte DMARC policy hebben we in onderzoek.

Er zijn verschillende pogingen van cybercriminaliteit waargenomen door Schiphol, dit staat ook vermeld in ons jaarverslag. Mede dankzij onze cyber securitymaatregelen hebben deze pogingen tot dusver geen impact gehad op onze dienstverlening. Schiphol heeft een nauwe samenwerking met het NCSC, zo wisselen we bijvoorbeeld bevindingen uit. Ook heeft Schiphol tot dusver geen incident hoeven melden conform de meldplicht WBNI.

Zembla bekeek het jaarverslag. "IT disruption" door een "cyber attack" wordt daarin genoemd als één van de top 10-risico's van Schiphol.

21. Stedin

Stedin en Enduris/DNWG zijn netbeheerders van het gas- en elektriciteitsnet in Zuid-Holland, Utrecht en Zeeland. Deze netten zijn onderdeel van de vitale energie-infrastructuur van het meest stedelijke gebied van Nederland. Het veilig maken en houden van deze netten zit in het DNA van ons bedrijf. We spannen ons optimaal in om onze systemen in stand te houden. We doen er alles aan om te voorkomen dat energievoorziening voor onze klanten en onze bedrijfsvoering in gevaar komen. Wij voeren regelmatig tests uit en monitoren het energienet 24/7u op eventuele bedreigingen en onze ruim 5000 medewerkers worden actief getraind om de organisatie weerbaarder te maken tegen cybercriminaliteit.

Er bestaan vele vormen van cybercriminaliteit. Ook wij hebben last van pogingen tot deze criminaliteit. Ondanks genomen maatregelen hebben ook wij in de praktijk er wel eens te maken dat er op een verkeerde link wordt geklikt of een besmet bestand wordt geopend. We beschikken over goed beveiligde systemen waardoor dergelijke acties in de kiem gesmoord worden en niet tot verdere schade leiden of hebben geleid.

We zijn op dit moment bezig met de implementatie van DMARC. DMARC is naast SPF en DKIM een extra beveiligingsmaatregel dat meehelpt in het voorkomen dat anderen digitale identiteitsfraude kunnen plegen en zich kunnen voordoen als medewerkers van Stedin of Enduris/DNWG. Digitale identiteitsfraude is slechts één facet van cybercriminaliteit, waarbij DMARC een extra laag bescherming geeft. Voor de overige vormen van cybercriminaliteit zijn andere gepaste maatregelen ingezet. We blijven ons continue inzetten met een breed en gelaagd scala aan maatregelen om alle vormen van cybercriminaliteit nu en in de toekomst tegen te gaan.

22. Tennet

TenneT is de landelijk netbeheerder van het hoogspanningsnet, de 'snelwegen' van ons elektriciteitsnetwerk. TenneT is actief in Nederland en een deel van Duitsland. Onze hoogspanningsnetten zijn onderdeel van de vitale energie-infrastructuur in Europa. Het veilig maken en houden van deze hoogspanningsnetten zit in het DNA van TenneT. We doen er alles aan om te voorkomen dat de elektriciteitsvoorziening voor onze klanten en onze bedrijfsvoering in gevaar komen. Wij voeren met regelmaat tests uit en monitoren het hoogspanningsnet 24/7u op eventuele

bedreigingen. Onze ruim 5000 medewerkers worden actief getraind om de organisatie weerbaar te houden tegen cybercriminaliteit.
Er bestaan vele vormen van cybercriminaliteit. Ook wij hebben last van pogingen tot deze criminaliteit. Ondanks genomen maatregelen hebben ook wij in de praktijk er wel eens mee te maken dat er op een verkeerde link wordt geklikt of dat er een besmet bestand wordt geopend. We beschikken over goed beveiligde systemen, goed opgeleide mensen en degelijke security-processen waardoor dergelijke acties niet tot verdere schade leiden of hebben geleid.
We blijven ons continue inzetten met een breed scala aan maatregelen om alle vormen van cybercriminaliteit nu en in de toekomst tegen te gaan. We focussen ons daarbij uiteraard op de hoogste risico's voor TenneT en vooral rondom de vitale energie-infrastructuur waar wij onderdeel van zijn. De door jullie genoemde technische middelen zijn slechts een onderdeel van dit brede scala aan maatregelen.

We zijn op dit moment bezig met de implementatie van DMARC en SPF. Digitale identiteitsfraude is slechts één facet van cybercriminaliteit, waarbij o.a. DMARC een extra laag bescherming geeft.

23. T-Mobile

T-Mobile heeft veiligheid hoog in het vaandel staan. Verschillende teams zijn dag en nacht aan het werk voor onze klanten én medewerkers om te zorgen voor een veilig netwerk, vertrouwelijke communicatie en veilig beheer van data en persoonsgegevens. Omdat we veilig gebruik van onze diensten voor onze klanten willen waarborgen en ook omdat we dat wettelijk verplicht zijn. We wapenen ons tegen externe invloeden om dat te bewerkstelligen en hebben daarover contact met verschillende instanties, waaronder het NCSC – dat als organisatie niet-bindende aanbevelingen afgeeft.

Onze beveiligingsstrategie berust op een serie maatregelen en beveiligingssystemen die samen een sterk geheel vormen en veiligheid garanderen. We nemen onze processen continu onder de loep en voeren verbeteringen door waar nodig, om de veiligheid van onze klanten te waarborgen en ook in de toekomst ruimschoots te voldoen aan wettelijke verplichtingen.

Helaas kunnen wij geen uitspraken doen over gevallen van cybercriminaliteit maar we willen u wel wijzen op de meldingsplicht die wij als bedrijf hebben.

24. Uniper

Uniper wil BNNVara danken voor de gelegenheid om op het thema cyberveiligheid in te gaan. Het gaat bij de genoemde voorbeelden niet om een zeer kritisch risico ten aanzien van onze reguliere werkzaamheden in de energiesector. Uiteraard nemen wij alle opmerkingen wel zeer serieus en dit onderwerp heeft onze continue aandacht. Over specifieke bestaande of nieuwe maatregelen hieromtrent doen wij geen uitspraken. Ook doen wij geen mededelingen over het aantal cybercrime incidenten. Wij kunnen wel bevestigen dat onze maatregelen regelmatig gevalideerd en waar nodig aangepast worden.

25. Vattenfall

1. Kunt u aangeven waarom de betreffende beveiligingsmaatregel (strikte DMARC-policy) niet is genomen?
DMARC is een van de opties waarmee je kunt verifiëren dat de persoon die de e-mail verzendt, is wie hij zegt dat hij is. We zijn bezig met het verder instellen van DMARC voor al onze domeinen (68% van onze domeinen is al volledig ingesteld). Op dit moment gebruiken we daarnaast geavanceerde technologie en veelgebruikte protocollen om ons te beschermen tegen phishing-aanvallen. Door deze maatregelen vormt de nog niet volledige implementatie van DMARC geen direct risico voor Vattenfall, maar wij zien wel de meerwaarde en voeren zoals gezegd het protocol verder uit.

2. Zijn er in de afgelopen vijf jaar (pogingen tot) cybercriminaliteit geweest bij uw organisatie?
We begrijpen dat u hierom vraagt, maar alle informatie of inzichten die we u zouden geven over onze beveiliging ondermijnt die beveiliging. Daarom doen wij hier geen concrete uitspraken over, maar elk bedrijf is een continu doelwit van cybercrime en is hierop voorbereid (of zou dat moeten zijn).

3. Zo ja, om welke vorm(en) van cybercriminaliteit ging het? (bijvoorbeeld hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)
Zie 2.

4. Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?
Zie 2.

5. Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?
Ja, sommige van onze bedrijfsonderdelen vallen onder de WBNI. We reageren niet op individuele meldingen.

6. Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?
Nee, het NCSC heeft ons niet actief benaderd over het niet volledig configureren van het DMARC-protocol op ons @vattenfall.com-domein.

7. Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja welke? Zo nee, waarom niet?
Zoals eerder aangegeven, rollen we DMARC de komende maanden al uit naar 100% voor onze domeinen.

26-38. Veiligheidsregio's Amsterdam, Brabant-Noord, Friesland, Gelderland-Midden, Gelderland-Zuid, Groningen, IJsselland, Limburg-Noord, Midden- en West-Brabant, Rotterdam-Rijnmond, Utrecht, Zeeland en Zuid-Limburg

Het televisieprogramma Zembla heeft via e-mail kenbaar gemaakt aandacht te hebben voor de cybersecurity van veiligheidsregio's en heel specifiek voor de beveiliging van mailservers. Een aantal veiligheidsregio's heeft een e-mailbericht ontvangen, waarin zij in kennis worden gesteld van een issue met de beveiliging van hun mailserver en gevraagd worden om een aantal vragen daarover te beantwoorden. Deze vragen zijn identiek en gericht op cybersecuritymaatregelen en de samenwerking tussen veiligheidsregio's en het NCSC. Om voornoemde redenen zal VR-ISAC de beantwoording gecentraliseerd en thematisch ter hand nemen. VR-ISAC is het sectorale inlichtingencentrum op het gebied van cybersecurity en cyberdreigingen van de 25 veiligheidsregio's en het Instituut Fysieke Veiligheid (IFV).

Hoewel veiligheidsregio's onderdeel zijn van de nationale crisisstructuur, behoren veiligheidsregio's formeel gezien niet tot de vitale sectoren of vitale aanbieders. Betrokkenheid bij één of meer vitale processen kent geen automatisme voor wat betreft de toekenning van de status "vitaal". Veiligheidsregio's hebben echter op eigen initiatief informatiebeveiliging prioriteit gegeven in hun samenwerking en hebben gezamenlijk een vakgroep informatieveiligheid opgericht. Deze vakgroep heeft een gemeenschappelijk normenkader voor informatiebeveiliging vastgesteld en een systeem van collegiale toetsingen op die normen ingericht.

Er is EU-wetgeving in ontwikkeling (NIS2) waarin overheidsinstanties per definitie vitaal worden verklaard: Nieuwe EU-cyberbeveiligingsstrategie en nieuwe regels om fysieke en digitale kritieke entiteiten veerkrachtiger te maken - Vragen en antwoorden - Europa Nu (europa-nu.nl).

Veiligheidsregio's zetten dus al een aantal jaren met prioriteit in op cybersecurity maar hebben daarbij vaak nog (deels) te maken met een complex ICT-landschap, dat bij de vorming van de veiligheidsregio's werd samengevoegd vanuit de verschillende gemeentelijk organisaties waaruit ze zijn ontvlochten. In de afgelopen jaren is, mede door het normenkader en collegiale toetsingen, breed ingezet op kwalitatieve verbetering en modernisering van het ICT-landschap bij de veiligheidsregio's.

Verbetering kost tijd en het tempo van de verbetering wordt voornamelijk bepaald door prioritering van verbeterprojecten en aanbestedingsprocedures die tijd kosten. Veiligheidsregio's zijn dit jaar gestart met een versnellingsprogramma informatieveiligheid om het tempo nog verder te verhogen.

Alle veiligheidsregio's hebben beveiligingsmaatregelen geïmplementeerd op hun mailservers, een aantal veiligheidsregio's heeft echter nog niet het volledige spectrum beveiligingsmaatregelen DKIM/SPF/DMARC geïmplementeerd. Belangrijk om daarbij te vermelden is dat de veiligheidsregio's, die nog niet volledig aan de full-spectrum beveiliging voor mailservers voldoen, vlak vóór of middenin een migratietraject zitten waarin het ICT-landschap, inclusief de beveiliging van mailservers, wordt verbeterd en vernieuwd. Veiligheidsregio's wegen zelf de risico's af van de huidige situatie tegen de ontwikkelingen die al zijn ingezet in migratietrajecten naar een nieuwer en veiliger ICT-landschap.

Veiligheidsregio's zijn, net als iedere andere organisatie, blootgesteld aan cyberrisico's, waaronder cybercrime. Zonder in te gaan op specifieke incidenten kan worden gemeld dat op dagelijkse basis bij alle veiligheidsregio's pogingen worden gedetecteerd en gestopt die erop gericht zijn om in netwerken of systemen binnen te dringen, systemen te besmetten met malware of financiële transacties proberen uit te lokken.

Eén incident bij een veiligheidsregio heeft geleid tot een cybercrisis en deze is ook publiek gemaakt: Veiligheidsregio in Gelderland getroffen door ransomware | NU - Het laatste nieuws het eerst op NU.nl.
Er is van dit incident een uitgebreide evaluatie beschikbaar: Evaluatie gijzelsoftware VNOG (ifv.nl).

Door de instelling van de VR-ISAC hebben veiligheidsregio's en het IFV een formele informatie-uitwisseling met het NCSC ingericht. Details daarover kunnen niet worden gegeven, maar in algemene zin betreft het vertrouwelijke uitwisseling van informatie met betrekking tot cyberdreigingen en cyberincidenten. Daarbij stelt de wbni de kaders aan de informatie die het NCSC aan VR-ISAC mag verstrekken. VR-ISAC vertaalt informatie van het NCSC naar handelingsperspectief voor de veiligheidsregio's en stemt beeldvormend af met andere partijen binnen het Landelijk Dekkend Stelsel.

39. VodafoneZiggo

VodafoneZiggo verbetert beveiliging e-mail

Per 1 oktober 2021 zijn de e-mailsystemen van VodafoneZiggo beter beveiligd met de zogeheten DMARC-beveiliging. VodafoneZiggo werkt voortdurend aan de beveiliging van haar netwerk en systemen. Daarom laten we de beveiliging van onze systemen geregeld onderzoeken door experts.

Enige maanden geleden zagen we tekortkomingen in de e-mail beveiliging en zijn we begonnen met het invoeren van de DMARC-beveiliging, waaronder voor het domein '@vodafoneziggo.com'. Veel interne processen en systemen gebruiken dit domein. Om storingen te voorkomen moest de invoering hiervan daarom zorgvuldig gebeuren en dat kost tijd. Nu zijn dit domein en andere domeinen zoals '@ziggo.nl' en '@vodafone.nl' beveiligd met DMARC. Dit verbetert de beveiliging van onze e-mailsystemen en voorkomt dat nep e-mails kunnen worden verstuurd uit naam van ons bedrijf.

VodafoneZiggo is Zembla erkentelijk voor het waarschuwen voor dit soort beveiligingsproblemen op het internet. Cybercriminaliteit is een groot maatschappelijk probleem dat permanent aandacht verdient. Daarom werken we samen met andere partijen in de markt en verschillende overheidsinstanties in de bestrijding hiervan.

1) Kunt u aangeven waarom betreffende veiligheidsmaatregel (strikte DMARC-policy) niet is genomen?

Per 1 oktober 2021 zijn de e-mailsystemen van VodafoneZiggo beter beveiligd met de zogeheten DMARC-beveiliging. We werken voortdurend aan de beveiliging van ons netwerk en systemen. Daarom laten we de beveiliging van onze systemen geregeld onderzoeken door experts. Enige maanden geleden zagen we tekortkomingen in de e-mail beveiliging en zijn we begonnen met het invoeren van de DMARC-beveiliging, waaronder voor het domein '@vodafoneziggo.com'. Veel interne processen en systemen gebruiken dit domein. Om storingen te voorkomen moest de invoering hiervan daarom zorgvuldig gebeuren en dat kost tijd. Nu zijn dit domein en andere domeinen zoals '@ziggo.nl' en '@vodafone.nl' beveiligd met DMARC. Dit verbetert de beveiliging van onze e-mailsystemen en voorkomt dat nep e-mails kunnen worden verstuurd uit naam van ons bedrijf.

2) Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?

Net als veel andere organisaties hebben wij ook te maken met pogingen tot cybercriminaliteit. Wij monitoren onze systemen daarom continu op mogelijke dreigingen. Gespecialiseerde teams die gebruikmaken van geavanceerde software grijpen in wanneer onbevoegden onze systemen willen misbruiken. We trainen onze medewerkers in het alert zijn op cybercriminaliteit. Daarnaast werken we samen met andere partijen in de markt en verschillende overheidsinstanties in de bestrijding van cybercriminaliteit.

3) Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?

Wij hebben de pogingen tot het plegen van cybercriminaliteit kunnen voorkomen.

4) Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)

Wij monitoren onze systemen continu op mogelijke dreigingen. We hebben verschillende pogingen tot het plegen van cybercriminaliteit gezien en die kunnen voorkomen.

5) Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?

Wij zijn een vitale aanbieder omdat wij een dienst aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. Wij melden incidenten daarom bij het Nationaal Cyber Security Centrum conform de Wet beveiliging netwerk- en informatiesystemen (Wbni).

6) Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?

Wij kunnen niet spreken namens het Nationaal Cyber Security Centrum. Voor vragen over de activiteiten van het NCSC verwijzen wij u door naar hen.

7) Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?

Per 1 oktober 2021 zijn de e-mailsystemen van VodafoneZiggo beter beveiligd met de zogeheten DMARC-beveiliging. We werken voortdurend aan de beveiliging van ons netwerk en systemen. Daarom laten we de beveiliging van onze systemen geregeld onderzoeken door experts. Enige maanden geleden zagen we tekortkomingen in de e-mail beveiliging en zijn we begonnen met het invoeren van de DMARC-beveiliging, waaronder voor het domein '@vodafoneziggo.com'. Veel interne processen en systemen gebruiken dit domein. Om storingen te voorkomen moest de invoering hiervan daarom zorgvuldig gebeuren en dat kost tijd. Nu zijn dit domein en andere domeinen zoals '@ziggo.nl' en '@vodafone.nl' beveiligd met DMARC. Dit verbetert de beveiliging van onze e-mailsystemen en voorkomt dat nep e-mails kunnen worden verstuurd uit naam van ons bedrijf.

40. Waterbedrijf Groningen

Goed om te weten is dat Waterbedrijf Groningen en WMD Drinkwater een gezamenlijke ICT-afdeling hebben. Onze antwoorden komen dan ook overeen.

Drinkwaterbedrijven vinden het belangrijk om veilige diensten te leveren. Ondanks alle zorg en inzet hiervoor, kúnnen er kwetsbaarheden in de beveiliging zitten (of een vermoeden daartoe).

Op de websites van drinkwaterbedrijven wordt het melden van eventuele kwetsbaarheden door externe partijen, zoals The Internet Cleanup Foundation, aangemoedigd via de hiervoor bedoelde processen. Meldingen van eventuele kwetsbaarheden helpen ons om te kijken waar verbeteringen mogelijk zijn. De sector voert dan ook sinds 2014 een zogenoemd Coördinated Vulnerability Disclosure (CVD) beleid (gebaseerd op de Leidraad van het NCSC) . Bedrijven nemen de melding in behandeling (Resposible Disclosure) en nemen binnen een aantal werkdagen contact op met de melder om afspraken te maken over een redelijke herstelperiode (indien dat van toepassing is) en een eventuele gecoördineerde publicatie van het beveiligingslek.

Vragen

1. Kunt u aangeven waarom betreffende veiligheidsmaatregel (DMARC) niet is genomen?

Het NCSC geeft adviezen en handelingsperspectief aan vitale bedrijven, waaronder de tien Nederlandse drinkwaterbedrijven, over kwetsbaarheden en dreigingen. Als drinkwatersector acteren wij weloverwogen en proactief op gedegen eigen risicoanalyses, wettelijke eisen en adviezen van het NCSC.

Waterbedrijf Groningen heeft haar ICT afdeling (die zij deelt met WMD Drinkwater in Drenthe) opdracht gegeven om te kijken naar uw op- en aanmerkingen. Daarop is een Responsible Disclosure procedure opgestart. We gaan als waterbedrijven uiterst zorgvuldig om met cyberveiligheid. Als er kwetsbaarheden zijn, dan nemen we die serieus. We hebben naar aanleiding van uw onderzoek en melding geconstateerd dat er verbeteringen mogelijk zijn. Die verbeteringen zijn doorgevoerd.

2. Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?

In het Cyber Security Beeld Nederland (CSBN) is te lezen dat drinkwaterbedrijven o.a. worden geconfronteerd met pogingen tot ransomware- en phishingaanvallen in de kantoorautomatiseringsomgeving. Wij voeren actief beleid om ons daartegen te wapenen.

Ook staat in het Cyber Security Beeld Nederland (CSBN) dat gerichte aanvallen op de vitale processen (waaronder de drinkwatervoorziening) in Nederland niet zijn waargenomen.

3. Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)

Zie vraag 2.

4. Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?

Vanuit beveiligingsoptiek is specifieke informatie over pogingen tot cybercriminaliteit vertrouwelijk.

5. Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?

Ja, de tien Nederlandse drinkwaterbedrijven zijn aangewezen tot aanbieders van essentiële diensten (AED's) en vallen derhalve onder de Wbni. Op basis van de Wbni hebben drinkwaterbedrijven een meldplicht bij het NCSC en de sectorale toezichthouder, de ILT.

De wettelijke meldplicht op basis van de Wbni betreft incidenten en/of inbreuken die aanzienlijke gevolgen (kunnen hebben) voor de continuïteit van de vitale dienst. Bij drinkwaterbedrijven gaat het hierbij om de drinkwatervoorziening. De melding van The Internet Cleanup Foundation heeft daar geen betrekking op.

6. Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?

Het NCSC heeft in 2015 een factsheet gepubliceerd over bescherming van domeinnamen tegen phishing. Zoals bij vraag 1 staat uiteengezet, nemen drinkwaterbedrijven op basis van mogelijke risico's maatregelen en maken een afweging om al dan niet aanvullende maatregelen te treffen. Drinkwaterbedrijven zijn immers zelf verantwoordelijk voor bescherming van beschikbaarheid, integriteit en vertrouwelijkheid van hun data en systemen én het managen van evt. risico's rondom deze data en systemen.

7. Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?

Meldingen van eventuele kwetsbaarheden in de beveiliging van onze diensten nemen wij altijd serieus. Dat geldt ook voor het onderzoek van The Internet Cleanup Foundation. Naar aanleiding van de melding van The Internet Cleanup Foundation hebben we gekeken naar mogelijke verbeteringen. Zoals gemeld in het antwoord op vraag 1 hebben we deze doorgevoerd.

41. Westland Infra / Juva

Westland Infra Netbeheer verzorgt de distributie van elektriciteit en gas in de regio's Westland en Midden-Delfland en in een aantal voormalige private netten in het Rotterdamse havengebied. Wij zorgen als netwerkbedrijf voor efficiënte energie-infrastructuren met een hoge mate van veiligheid en beschikbaarheid. We streven naar zo min mogelijk uitval van ons net en doen er alles aan dat onze bedrijfsvoering niet in gevaar komt. We laten onze beveiliging regelmatig testen, scannen actief naar kwetsbaarheden in onze systemen en beoefenen de respons op incidenten. Bij al onze dagelijkse werkzaamheden staan kwaliteit en veiligheid hoog in het vaandel.

Wij trainen onze medewerkers regelmatig op cybercriminaliteit. Onze medewerkers zijn erop getraind om proactief verdachte mails met een verkeerde link te melden. En indien van toepassing informeren wij de juiste instanties. Onze systemen zijn goed beveiligd, waardoor pogingen tot cybercriminaliteit op tijd ontdekt en aangepakt worden.

We maken onze organisatie weerbaar tegen de diverse vormen van cybercriminaliteit. We werken op dit moment aan de implementatie van DMARC, één van de maatregelen die bescherming geeft tegen

ongeautoriseerd mailen namens onze domeinen. We werken continue aan verbeteringen en aanpassingen op de maatregelen om cybercriminaliteit nu en in de toekomst tegen te gaan.

42. WMD / Drinkwater Drenthe

De mail van Waterbedrijf Groningen en die van ons komt overeen.

Drinkwaterbedrijven vinden het belangrijk om veilige diensten te leveren. Ondanks alle zorg en inzet hiervoor, kúnnen er kwetsbaarheden in de beveiliging zitten (of een vermoeden daartoe).

Op de websites van drinkwaterbedrijven wordt het melden van eventuele kwetsbaarheden door externe partijen, zoals The Internet Cleanup Foundation, aangemoedigd via de hiervoor bedoelde processen. Meldingen van eventuele kwetsbaarheden helpen ons om te kijken waar verbeteringen mogelijk zijn. De sector voert dan ook sinds 2014 een zogenoemd Coördinated Vulnerability Disclosure (CVD) beleid (gebaseerd op de Leidraad van het NCSC) . Bedrijven nemen de melding in behandeling (Resposible Disclosure) en nemen binnen een aantal werkdagen contact op met de melder om afspraken te maken over een redelijke herstelperiode (indien dat van toepassing is) en een eventuele gecoördineerde publicatie van het beveiligingslek.

Hieronder de antwoorden op je vragen:

Vragen

1. Kunt u aangeven waarom betreffende veiligheidsmaatregel (DMARC) niet is genomen?

Het NCSC geeft adviezen en handelingsperspectief aan vitale bedrijven, waaronder de tien Nederlandse drinkwaterbedrijven, over kwetsbaarheden en dreigingen. Als drinkwatersector acteren wij weloverwogen en proactief op gedegen eigen risicoanalyses, wettelijke eisen en adviezen van het NCSC.

Drinkwaterbedrijf WMD heeft haar ICT afdeling de opdracht gegeven om te kijken naar uw op- en aanmerkingen. Daarop is een Responsible Disclosure procedure opgestart. We gaan als waterbedrijven uiterst zorgvuldig om met cyberveiligheid. Als er kwetsbaarheden zijn, dan nemen we die serieus. We hebben naar aanleiding van uw onderzoek en melding geconstateerd dat er bij WMD verbeteringen mogelijk zijn. Die verbeteringen zijn doorgevoerd.

2. Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?

In het Cyber Security Beeld Nederland (CSBN) is te lezen dat drinkwaterbedrijven o.a. worden geconfronteerd met pogingen tot ransomware- en phishingaanvallen in de kantoorautomatiseringsomgeving. Wij voeren actief beleid om ons daartegen te wapenen. Ook staat in het Cyber Security Beeld Nederland (CSBN) dat gerichte aanvallen op de vitale processen (waaronder de drinkwatervoorziening) in Nederland niet zijn waargenomen.

3. Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)

Zie vraag 2.

4. Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?

Vanuit beveiligingsoptiek is specifieke informatie over pogingen tot cybercriminaliteit vertrouwelijk.

5. Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?

Ja, de tien Nederlandse drinkwaterbedrijven zijn aangewezen tot aanbieders van essentiële diensten (AED's) en vallen derhalve onder de Wbni. Op basis van de Wbni hebben drinkwaterbedrijven een meldplicht bij het NCSC en de sectorale toezichthouder, de ILT. De wettelijke meldplicht op basis van de Wbni betreft incidenten en/of inbreuken die aanzienlijke gevolgen (kunnen hebben) voor de continuïteit van de vitale dienst. Bij drinkwaterbedrijven gaat het hierbij om de drinkwatervoorziening. De melding van The Internet Cleanup Foundation heeft daar geen betrekking op.

6. Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?

Het NCSC heeft in 2015 een factsheet gepubliceerd over bescherming van domeinnamen tegen phishing. Zoals bij vraag 1 staat uiteengezet, nemen drinkwaterbedrijven op basis van mogelijke risico's maatregelen en maken een afweging om al dan niet aanvullende maatregelen te treffen. Drinkwaterbedrijven zijn immers zelf verantwoordelijk voor bescherming van beschikbaarheid, integriteit en vertrouwelijkheid van hun data en systemen én het managen van evt. risico's rondom deze data en systemen.

7. Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?

Meldingen van eventuele kwetsbaarheden in de beveilig van onze diensten nemen wij altijd serieus. Aan de hand van het onderzoek van The Internet Cleanup Foundation hebben we gekeken naar mogelijke verbeteringen. Zoals gemeld in het antwoord op vraag 1 hebben we deze doorgevoerd.

43. WML / Drinkwater Limburg

Drinkwaterbedrijven vinden het belangrijk om veilige diensten te leveren. Ondanks alle zorg en inzet hiervoor, kúnnen er kwetsbaarheden in de beveiliging zitten (of een vermoeden daartoe). Meldingen van eventuele kwetsbaarheden helpen ons om te kijken waar verbeteringen mogelijk zijn. De sector voert dan ook sinds 2014 een zogenoemd Coördinated Vulnerability Disclosure (CVD) beleid (gebaseerd op de Leidraad van het NCSC). Bedrijven nemen de melding in behandeling en nemen binnen een aantal werkdagen contact op met de melder om afspraken te maken over een redelijke herstelperiode (indien dat van toepassing is) en een eventuele gecoördineerde publicatie van het beveiligingslek.

Vragen

1. Kunt u aangeven waarom betreffende veiligheidsmaatregel (DMARC + DKIM) niet is genomen?

Het NCSC geeft adviezen en handelingsperspectief aan vitale bedrijven, waaronder de tien Nederlandse drinkwaterbedrijven, over kwetsbaarheden en dreigingen. Als drinkwatersector acteren wij weloverwogen en proactief op gedegen eigen risicoanalyses, wettelijke eisen en adviezen van het NCSC. WML treft zelf, los van deze adviezen, proactief beveiligingsmaatregelen. Op een dieper niveau heeft WML de aanvullende beveiligingsmaatregelen geïmplementeerd. Onze eigen PDCA-cyclus heeft ertoe geleid dat we de afgelopen periode de implementatie van de beveiligingsmaatregelen op het hoogste niveau hebben onderzocht. De tussenresultaten van dit proces zijn positief en implementatie is gepland op korte termijn.

2. Zijn er de afgelopen vijf jaar (pogingen tot) cybercrime geweest bij uw organisatie?

In het Cyber Security Beeld Nederland (CSBN) over 2020 is te lezen dat drinkwaterbedrijven onder andere worden geconfronteerd met pogingen tot ransomware- en phishingaanvallen in de kantoorautomatiseringsomgeving. Wij voeren actief beleid om ons daartegen te wapenen.

Ook staat in het Cyber Security Beeld Nederland (CSBN) dat gerichte aanvallen op de vitale processen (waaronder de drinkwatervoorziening) in Nederland niet zijn waargenomen. Dat geldt ook voor WML in 2021.

3. Zo ja, om welke vorm(en) van cybercrime ging het? (bijv. hacking, malware, CEO-fraude, spoofing, spear phishing, datadiefstal, Ddos-aanvallen, ransomware, etc.)

Zie vraag 2.

4. Zo ja, in hoeverre waren die pogingen succesvol? Wat was de materiële en immateriële schade?

Zie vraag 2.

5. Behoort uw organisatie tot de vitale aanbieders zoals deze in de Wbni staan geformuleerd? Zo ja, is een eventueel incident gemeld bij het NCSC?
Ja, de tien Nederlandse drinkwaterbedrijven zijn benoemd tot aanbieders van essentiële diensten (AED's) en vallen derhalve onder de Wbni. Op basis van de Wbni hebben drinkwaterbedrijven een meldplicht bij het NCSC en de sectorale toezichthouder, de ILT.
De wettelijke meldplicht op basis van de Wbni betreft incidenten en/of inbreuken die aanzienlijke gevolgen (kunnen hebben) voor de continuïteit van de vitale dienst. Bij drinkwaterbedrijven gaat het hierbij om de drinkwatervoorziening. Incidenten hebben zich niet voorgedaan, zie ook vraag 2.

6. Heeft het NCSC uw organisatie ooit actief benaderd of individueel gewaarschuwd voor het ontbreken van deze veiligheidsmaatregel(en) in uw mailserver?

WML is niet gewaarschuwd door het NCSC. WML treft zelf proactief veiligheidsmaatregelen. Drinkwaterbedrijven zijn immers zelf verantwoordelijk voor bescherming van beschikbaarheid, integriteit en vertrouwelijkheid van hun data en systemen én het managen van eventuele risico's rondom deze data en systemen.

7. Bent u van plan maatregelen te nemen n.a.v. de onderzoeksresultaten? Zo ja, welke? Zo nee, waarom niet?

Meldingen van eventuele kwetsbaarheden in de beveiliging van onze diensten nemen wij altijd serieus. Dat geldt ook voor het onderzoek van The Internet Cleanup Foundation. We hebben de resultaten van het onderzoek beoordeeld en kunnen u melden dat de benodigde aanvullende beveiligingsmaatregelen op korte termijn ook op het hoogste niveau geïmplementeerd zullen zijn.