WAT ZOU JIJ DOEN?

'Als het een keer misgaat, moeten we elkaar weten te vinden'

Raymond Knops, Staatssecretaris van BZK

INHOUD

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

NL DIGIbeter

INFORMATIE BEVEILIGINGS DIENST

UNIE VAN WATERSCHAPPEN

VNG

Ministerie van Economische Zaken en Klimaat

Interprovinciaal Overleg ipo

CIP centrum informatiebeveiliging en privacybescherming

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

ICTU

COLOFON

Eindredactie en coördinatie Eric Went en Jos van Duinen **Redactie** Michelle Alberda, Nynke Dijkstra, Annemarie Foekema, Robin van Gerwen, Dirk Goet, Noah Grootscholten, Kevin van Haaren, Andrea van den Hooff, Sophie Keizer, Elsemieke Kunst, Robin Martinot, Suzanne Mos, Victor Trees, Jorrit Tromp, Niki Versteeg, Jona van der Wel, Elise Wendt en Juline Wilkinson
Fotografie Loes van Gameren, Monique Shaw **Illustratie** ferrytekent.nl **Vormgeving** John Stelck

MAGAZINE ON THE SPOT

Cyberincidenten vormen een steeds grotere bedreiging voor overheden, bedrijven en burgers. Deze incidenten kunnen desastreuze gevolgen hebben voor de dienstverlening. Daarom is het belangrijk dat de overheid haar informatieveiligheidsbeleid op orde heeft. Maar als er dan toch iets misgaat, is de overheid dan wel voldoende voorbereid? Weten we wat we moeten doen en welke instrumenten we moeten inzetten op het moment dat een cyberincident uitgroeit tot een cybercrisis?

‘Be prepared for the worst’ en daarom blijft het verhogen van de informatieveiligheid binnen overheidsorganisaties de komende jaren een belangrijk speerpunt van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Zo wordt er onder ander gewerkt aan een aantal overheidsbrede maatregelen, zoals de Baseline Informatieveiligheid voor alle overheden, Incident response capaciteit en het oefenen met cyberincidenten. Digitalisering brengt immers veel kansen met zich mee, maar tegelijkertijd is er blijvende aandacht nodig voor de risico’s.

Cyberincidenten zijn lastig te voorspellen en te voorkomen en voor het oplossen van dergelijke incidenten is samenwerking van essentieel belang. Overheidsbrede samenwerking is onontbeerlijk en daarom hecht ik aan het belang van oefenen. Wanneer het dan een keer misgaat, weten we elkaar te vinden en zijn we beter in staat in te spelen op de incidenten die zich voordoen.

Om die reden vond op 28 oktober, tijdens de Europese maand van de cybersecurity, de overheidsbrede oefening ‘Wat zou jij doen?’ plaats. Dit magazine bevat de hoogtepunten en de geleerde lessen van deze bijeenkomst.

Door te oefenen kunnen we beter inspelen aan de voorkant zodat je bent voorbereid wanneer het een keer echt misgaat. Ik hoop daarnaast dat de verschillende bestuurslagen na deze dag elkaar beter en vaker weten te vinden om kennis te delen, te netwerken en vooral handvatten te krijgen voor wanneer het dreigt mis te gaan.

Raymond Knops
Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Bron programmaboekje overheidsbrede cyberoefening
www.weerbaredigitaleoverheid.nl

ZIJN WE ER KLAAR VOOR?

Wat zijn de grootste dreigingen om ons zorgen over te maken? En wat doen we als het zover komt? Vier vertegenwoordigers van de overheid buigen zich tijdens de plenaire discussie over deze vragen.

‘Houd die voorkant dicht’

“Het IT systeem in onze gemeente is recent gehackt. We hebben het complete systeem vervolgens opnieuw opgebouwd. Een verschrikkelijk besluit, we waren een dag gesloten en nauwelijks bereikbaar. Ik heb hier twee lessen uit geleerd; houd die voorkant dicht, en denk van tevoren na over je weerbaarheid in het geval van een cyberincident.”

Sebastiaan van ’t Erve

Burgemeester van Lochem

‘Alleen veilige hard-en software aanschaffen’

“Wil je als samenleving profiteren van de economische groei dan is cyberveiligheid een voorwaarde. Daarom moeten we mensen stimuleren om alleen veilige soft- en hardware aan te schaffen. Door ze goed voor te lichten, maar ook door verkeerde spullen te onderscheppen, en slimme apparaten te certificeren.”

Jos de Groot

Directeur Digitale Economie, ministerie van Economische Zaken en Klimaat

‘Je kunt nooit genoeg doen’

“Informatieveiligheid staat hoog op onze agenda. Je kunt nooit genoeg doen aan het voorkomen van cybercriminaliteit. Het onderwerp moet prominent op de tafel en in de agenda van de bestuurders blijven.”

Marieke van Wallenburg

DG Overheidsorganisatie, ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Wees voorbereid

“We moeten Nederland veilig houden voor een digitale black-out. Dit kan alleen als we onszelf beschermen en voorbereiden. Door het delen van kennis en expertise met publieke en private partijen versterken we onze slagkracht. Wees voorbereid op dreigingen en weet wat je echt wilt beschermen.“

Patricia Zorko

Plaatsvervangend NCTV, ministerie van Justitie en Veiligheid

De deelnemers aan de plenaire cyberoefening speelden een rol voor een fictieve organisatie.

DETECT

Een aantal tunnels op belangrijke wegen in Hilversum, Veenendaal en Utrecht loopt onder water. De oorzaak is niet duidelijk, er lijkt geen verband tussen de incidenten. Op sociale media delen burgers foto's van de veroorzaakte verkeersopstoppingen. Ook vanuit andere locaties in het gebied komen meldingen binnen. Niet alle waterschappen zien wat er precies aan de hand is. Het is niet duidelijk waar de problemen door veroorzaakt worden, en wie er verantwoordelijk voor is. De waterschappen besluiten na overleg over te stappen naar handbediening.

AAN DE CRISISTAFEL

Frans Backhuijs
Burgemeester van Nieuwegein
Steven van de Looij
Directeur Veiligheidsregio Noord-Holland
Henk Heijnemans
Manager Bedrijfsvoering provincie Utrecht
Wouter Slob
Secretaris-Directeur Waterschap Zuiderzeeland

FRANS BACKHUIJS: "In eerste instantie ga ik op gemeentelijk niveau aan de slag. Ik laat mijn beleidsteam uitzoeken waar de wateroverlast vandaan komt. Vervolgens ga ik onderzoeken hoe ik mijn burgers kan informeren, ook al kennen we de oorzaak van het probleem nog niet. Het gaat erom de burgers zo snel mogelijk een handelingsperspectief te bieden."
STEVEN VAN DE LOOIJ: "Wij richten ons in deze fase op ons dagelijks werk, het wegpompen van water. En omdat het meer lijkt op een reguliere overstroming, gaan we contact zoeken met de burgemeester en de waterschappen."
HENK HEIJNEMANS: "Allereerst gaan we op zoek naar de feiten en gaan we schakelen met de veiligheidsregio, op zoek naar hulp en kennis."
WOUTER SLOB: "Dat is ook onze eerste stap, daarnaast zoeken we contact met de provincie en de gemeente. Het is belangrijk om te weten wat er daadwerkelijk aan de hand is. Tot die tijd kiezen wij ervoor om niets te doen."

De verschillende betrokken organisaties schalen volgens protocol op en beschrijven hun bevindingen in het LCMS-systeem. Doordat hier alle informatie bij elkaar komt wordt langzaam duidelijk dat er een relatie bestaat tussen de verschillende meldingen. Er wordt niet uitgesloten dat er ook een digitale component in het spel is. Het CERT (Computer Emergency Response Team) van de Waterschappen vertrouwt het niet en gaat schakelen met het SOC (Security Operations Center) van Rijkswaterstaat.

HET TEAM BREIDT ZICH UIT

Rob de Lange, CERT Waterschappen
Jeroen Schipper, CISO, Gemeente Den Haag
Nausikaa Efstratiades, Hoofd IBD

FRANS BACKHUIJS: "Nu is het moment om onze technische mensen in te schakelen om uit te zoeken wat er precies aan de hand is. Is hier sprake van een technisch probleem of van een hack?"
WOUTER SLOB: "Er blijken meer waterschappen betrokken in het verhaal. Er moet meer aan de hand zijn, we moeten uitzoeken wat dat is. We moeten alle kennis benutten die voorhanden is, dus ook CASO (Cyber Advanced Support Operations) en de IBD (Informatiebeveiligingsdienst) inschakelen."
ROB DE LANGE: "Er zijn meerdere waterschappen betrokken in het verhaal, wij gaan proberen de coördinatie te pakken. De mensen van de IT-afdelingen van de verschillende waterschappen zetten we vervolgens aan het werk, zij beschikken over veel expertise om dit verder uit te zoeken."
JEROEN SCHIPPER: ""Wij nemen contact op met IBD, externe experts en leveranciers. Gaat het alleen om de gemalen of ook om meer IT-systemen? Uit alle informatie maken we een analyse en stellen we een plan op. Ik ga snel op zoek naar collega's binnen andere gemeenten die dezelfde problemen hebben en ga met hen overleggen. Hoe groter de groep, hoe meer kennis."
NAUSIKAA EFSTRATIADES: "We moeten inderdaad identificeren wat er aan de hand is maar het is ook zaak om rustig te blijven. Het is nog niet duidelijk of er andere gemeentelijke processen zijn geraakt. In deze fase is het van belang dat de impact en urgentie wordt bepaald. Wij vertegenwoordigen als IBD-CERT de belangen van de gemeente. Als CERT staan we klaar voor onze collega CERT's: we beschikken over een analysecapaciteit die zij kunnen benutten en wij kunnen alle gemeenten bereiken."
WOUTER SLOB: "We moeten de verschillende scenario's bekijken, ook de *worst case*. Behalve weerbaarheid is namelijk ook wendbaarheid zeer belangrijk."
STEVEN VAN DE LOOIJ: "Als het incident zich over meerdere gemeentes verspreidt moeten we naar een hogere opschaling. Dan komt ook de dijkgraaf in het verhaal. En de dijkgraaf heeft dezelfde bevoegdheden als de burgemeester. Maar wie heeft eigenlijk de leiding? Dat moeten we duidelijk hebben."

RESPOND

Het journaal meldt dat de storingen worden veroorzaakt door hackers die hebben ingebroken bij de waterschappen. De hackers melden zich via Twitter. Rijkswaterstaat en het Ministerie van infrastructuur en Waterstaat hebben intern en met elkaar afstemming gezocht. Ze willen geïnformeerd blijven over de voortgang maar bemoeien zich – ze kwalificeren het als een 'lokale aangelegenheid' – niet actief met de incidenten. Een belangrijke vraag die opkomt is: moeten we de pers te woord staan?

FRANS BACKHUIJS: "Het is goed om de pers op de hoogte te brengen van het feit dat er een probleem is en om burgers op te roepen om thuis te blijven als ze niet per se de deur uit moeten."
HENK HEIJNEMANS: "We gaan dit communiceren en vertellen daarbij dan ook wat we niet weten."
STEVEN VAN DE LOOIJ: "Er moet duidelijkheid komen over wat er aan de hand is en wat we aan het doen zijn. We moeten de burgers duidelijk informeren over wat ze moeten doen en wat niet. En als we het vermoeden hebben van opzet, moeten de collega's van het Openbaar Ministerie aan tafel komen om de vervolgprocessen voor te bereiden."
ROB DE LANGE: "Wij gaan het probleem beperken door het te isoleren en te identificeren. En we gaan uitzoeken of het gerucht van de hacker waar is; we willen het zeker weten."
JEROEN SCHIPPER: "Inderdaad, isoleren. En we moeten onderzoeken of ook andere netwerken zijn geïnfecteerd. Als dat het geval is dan moeten deze worden afgesloten. Ik wil

contact (laten) zoeken met de Hacker om meer informatie over de aanval te krijgen."
ROB DE LANGE: "Contact zoeken met de hacker is zeker wenselijk. We moeten weten wat er aan de hand is."
NAUSIKAA EFSTRATIADES: "De Nederlandse overheid heeft het NRN in het leven geroepen. Dat staat voor het Nationaal response Netwerk. Als er onvoldoende capaciteit aanwezig is bij de betrokken incident response teams kan dat netwerk aangesproken worden. We bieden onze hulp aan via het NCSC (Nationaal Cyber Security Centrum)."
WOUTER SLOB: "Wij kijken eerst naar wat we zelf kunnen besluiten. Waar dat niet kan moeten we om advies vragen. Daartoe schakelen we dan met het NCSC. En met het OM."
STEVEN VAN DE LOOIJ: "Ik denk dat we nu te veel tegelijk aan het doen zijn. Het is efficiënter als we het werk verdelen. In oorzaak, effecten en taken. Dan ontstaat er meer overzicht."

***'Er is een workaround*, een patch** om het probleem op te lossen'*

ROB DE LANGE: "We moeten dit delen als het schoon blijkt."
JEROEN SCHIPPER: "Ik wil weten of er meer is aangetast. Het feit dat er een kwetsbaarheid is gevonden in de IT omgeving die mogelijk gerelateerd is aan de crisis, geeft aan dat er een mogelijk verband is. Dit maakt de scope van het probleem ineens veel groter. We gaan nu dus alles checken: OT én IT omgeving. Naar bestuurders moet gecommuniceerd worden dat het misschien niet alleen de waterschappen heeft geraakt en dat we sommige processen daarom stil leggen. De informatie wordt gedeeld met het CERT en de IBD."
FRANS BACKHUIJS: "Ik zou van CISO's en van de IBD willen weten hoe groot de kans is dat andere systemen op kantoor geïnfecteerd zijn of worden. Is het tijd om alles uit te zetten? Liever dit aan de burgers uitleggen dan de boel laten escaleren."
JEROEN SCHIPPER: "Ik zou dit nu nog niet doen. Feitelijk weten we alleen nog maar iets op macroniveau."

De hacker bericht dat hij lid is van een actiegroep die een punt wil maken over de digitale kwetsbaarheid van de overheid. 112 wordt intussen platgebeld. Gaan we de patch uitrollen?

NAUSIKAA EFSTRATIADES: "We moeten alle gemeenten over de kwetsbaarheid van het systeem en de mogelijkheid van de patch informeren. De IBD voegt aan de waarschuwingen van het NCSC een advies toe gebaseerd op de gemeentelijke context"
FRANS BAKHUIJS: "De dijkgraaf moet de crisis binnen de waterschappen oplossen, ik als burgermeester sta aan de lat voor de maatschappelijke onrust. De veiligheidsregio is hier de verbindende factor."

* Een **workaround** wordt ingevoerd wanneer een ideale oplossing niet beschikbaar is of als een tijdelijke maatregel is ingevoerd om een computer probleem aan te pakken.
** Een softwarematige **patch** is een klein stukje software dat door de uitgever van software gebruikt wordt om fouten op te lossen of updates uit te voeren aan zijn software.

RECOVER

De fysieke dreiging is voorbij. Op de crisistafel ligt nu een IT-probleem; de patch blijkt niet toereikend en er zijn problemen met verouderde systemen.

JEROEN SCHIPPER: "Nu is het zaak stap voor stap door ons gehele netwerk te gaan. We kunnen naar een normaal niveau terugschalen als de specialisten groen licht hebben geven. Dan pas is het systeem veilig."
ROB DE LANGE: "Bij verouderde systemen spelen andere factoren mee, hier moeten we een risicoanalyse van laten maken."
NAUSIKAA EFSTRATIADES: "We moeten elkaar helpen. Cybersecurity kennis binnen de overheid is schaars. De kennis die we hebben moeten we met elkaar delen."
ROB DE LANGE: "En er moet forensisch onderzoek gedaan worden waaruit moet blijken of de waterschappen schoon zijn. Zodra er vreemde dingen worden gesignaleerd moeten deze gedeeld worden met de andere waterschappen.".
JEROEN SCHIPPER: "Wat verantwoordelijkheden betreft wordt het pas complex op het moment dat het om meerdere gemeenten of meerdere waterschappen gaat. Het besluit van een burgemeester moet goed gevoed worden vanuit alle betrokken partijen en instanties."
ROB DE LANGE: "Binnen de sector is duidelijk wie wat moet doen. Het probleem met cyber is dat je vaak niet zelf aan de knoppen zit, maar dat iemand anders, een deskundige dat doet."
NAUSIKAA EFSTRATIADES: "Er zijn meerdere verantwoordelijken binnen het crisisteam, maar het is van belang dat één persoon de lijnen uitzet en beslissingen neemt."

RECAP

Wat hebben we van de Overheidsbrede Cyberoefening 'Wat zou jij doen?' geleerd? En wat gaan we daar in de dagelijkse praktijk mee doen? Zeven reacties van deelnemers na afloop van de oefening.

'Inspirerende dag die energie geeft'

"Ik heb een workshop gegeven en daar veel nieuwe waardevolle contacten opgedaan. Ik heb ook workshops gevolgd en gemerkt dat er nog veel te leren valt. Dat vind ik waardevol; als je niet weet van het bestaan van iets dan kun je er ook niet induiken. De oefening was inspirerend en geeft energie. Je ziet dat je niet de enige bent die hiermee bezig is, dat het eigenlijk het hele land bezighoudt."

'Het is nodig dat we hier met alle overheden voor staan'

"Ik vind het prettig dat er vandaag geen partijen betrokken zijn die buiten de overheid acteren. Dat maakt het oefenen, overleggen en netwerken overzichtelijk. Niemand hier heeft commerciële belangen. Vandaag komen processen, mensen en systemen aan bod. Het is belangrijk dat we hier gezamenlijk met alle overheden voor staan. En hard nodig."

'Niet verdwalen in een technisch verhaal'

"Wat ik vandaag bevestigd zie, is dat de security-mensen niet dezelfde taal spreken als de crisisbeheersings-mensen. Een goede coördinator is nodig om niet te verdwalen in een technisch verhaal waarin je vergeet waarom je eigenlijk bij elkaar zit: een besluit nemen om de boel op orde te krijgen. Mooi aan vandaag vind ik dat er zoveel mensen bij elkaar zijn gekomen; het vergroot de bewustwording en het enthousiasme om samen verder aan de slag te gaan."

'Je kweekt hier écht awareness mee'

"Cybercriminelen zitten niet stil, wij moeten als overheid meters maken. Met de nadruk op oefenen. Een oefening als die van vandaag leert wat er kan gebeuren en waar verbeterpunten liggen. En je kweekt er écht awareness mee. De grote hoeveelheid overheidsorganisaties die betrokken zijn bij een cyberincident kunnen ervoor zorgen dat het een complex geheel wordt. Eén zwakke schakel aan de crisistafel kan een probleem veroorzaken voor alle andere organisaties."

'Goed om dit vaker te doen'

"Ik vond het interessant om de deskundigen van de verschillende organisaties die niet iedere dag samenwerken te zien worstelen met elkaar. Het pakte goed uit, het is volgens mij belangrijk om te oefenen. Het lijkt me goed om dit vaker te doen."

'Ook de menselijke kant is belangrijk'

"Oefenen is heel belangrijk, het maakt je weerbaar. We moeten ons dan niet beperken tot de technische kant, maar ons ook op de menselijke kant richten. Iedere medewerker kan een zwakke schakel zijn. Betrek alle lagen uit de organisatie bij een oefening. Je ziet een verschuiving. Vroeger waren we vooral gericht op preventie. Nu accepteren we dat er cyberdreigingen zijn en richten we ons op de weerbaarheid."

'Uitdaging om belevingswerelden bij elkaar te krijgen'

"We moeten nog veel leren, dat wordt vandaag bevestigd. Binnen een organisatie heb je verschillende crisisorganisaties. Waar de een zich met de fysieke wereld bezighoudt richt de ander zich op de tastbare wereld en is de volgende actief in de cyberwereld. Het is een uitdaging om deze verschillende belevingswerelden en organisaties bij elkaar te krijgen. Wat we doen is daarom absoluut noodzakelijk."

KOFFIE VERKEERD

In het risicomanagementspel 'Koffie verkeerd' zijn de spelers CISO's, FG's of privacy officers bij de Rijksdienst voor Koffie & Theezaken (RvTK). Zij beheren de gegevens van medewerkers van alle overheidsinstellingen. Bij iedere spelronde doen zich een of meerdere risico's voor, waarvoor spelers zich kunnen indekken met maatregelen die zij kunnen kopen.

De Rijksdienst voor Koffie- & Theezaken (RvKT) zorgt dat de overheid nooit zonder koffie en thee zit. Daartoe heeft het de beschikking over een geavanceerd voorraadbeheersysteem dat volgens het just-in-time-principe zorgt dat er altijd precies genoeg voorraad is. Exacte gegevens over gebruiksgetallen koffie en thee zijn – uiteraard – departementaal vertrouwelijke gegevens. Het inkoopproces van de RvKT gebruikt het Systeem voor de Ultieme InKopER (SUIKER). De RvKT doet binnen het Structureel Langjarig Onderzoeksprogramma Koffie- en Theedrinken (SLOKT) onderzoek naar (veranderende) voorkeuren en gebruiken. Conform de AVG zijn deze gegevens voor een deel bijzondere persoonsgegevens. Maar wat als zich daarbij telkens nieuwe risico's voordoen? Hoe anticipeer je dan?

Lessons learned

- Wees je bewust van de onverwachte zaken die kunnen gebeuren;
- Neem maatregelen om risico's te minimaliseren;
- Ga in gesprek met vakgenoten over de scenario's die kunnen plaatsvinden.

ZO MAKEN WE ONZE INKOOP VEILIG!

In de roadmap 'Inkoopeisen Cybersecurity Overheid' (ICO) is gewerkt aan een set van algemene voorwaarden en minimum inkoopeisen voor de gehele Rijksoverheid. Doel daarvan is om opdrachtgevers, inkopers en contractmanagers goede veiligheidseisen mee te kunnen geven bij het inkopen van digitaal veilige hard- en software.
Daarvoor zijn de volgende handreikingen beschikbaar: inkoopsegmenten gebaseerd op BIO thema's, handreiking inkoop ICO en de ICO-wizard. De ICO-wizard is een Excel-tool waarmee de inkoop eenvoudig getoetst kan worden aan de BIO-eisen.

Meer weten?

Bezoek de **cip.pleio.nl**, de website van **BIO** of de thema-uitwerkingen op het **forum BIO** en bij **NORA-online bij ISOR**.

CYBERKOMPAS BRENGT BEDREIGINGEN IN KAART

Het Cybersecuritybeeld Nederland (CSBN) 2019 biedt inzicht in huidige dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Het Cyberkompas, dat binnenkort online gaat, is een expertproduct dat kijkt naar trends en verwachtingen die van invloed zijn op de digitale veiligheid van Nederland in de nabije toekomst. Met behulp van het Cyberkompas kunnen informatiebeveiligers, zoals security officers en CISO's, anticiperen op waargenomen en verwachte ontwikkelingen.

Dit zijn belangrijke trends volgens CSBN:

- De grootste dreiging komt vanuit statelijke actoren: Rusland, China, Noord-Korea en Iran.
- Criminele dreiging neemt toe, omdat:
  - het uitvoeren van cybercrime laagdrempelig en aantrekkelijk is;
  - de pakkans heel klein is;
  - de vervolging zo complex is dat de kans op veroordeling ook heel klein is.
- Bedrijven betalen bovendien liever dan dat ze hun bedrijfsprocessen stilleggen als gevolg van *ransomware**.
- De digitale weerbaarheid is niet overal op orde, omdat niet duidelijk is dat de kosten ruimschoots opwegen tegen de baten van het voorkomen van een cyberaanval. Pas na een incident gaan bedrijven hun beveiliging opschroeven.

Het Cyberkompas is een hulpmiddel waarmee je kunt nagaan wat binnen jouw bedrijf of sector de bedreigingen zijn en waar je jezelf weerbaarder kunt maken. Het NCSC organiseert workshops om met het Cyberkompas aan de slag te gaan.

*Ransomware is een programma dat een computer (of gegevens die erop staan) blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te 'bevrijden'

WATERKETEN VERGROOT DIGITALE WEERBAARHEID

Het Bestuursakkoord Water (BAW) heeft ertoe geleid dat diverse waterketenpartners de handen ineen hebben geslagen. Doel is een gezamenlijke cybersecurity ketenaanpak, gericht op procesautomatisering in de watersector. Het doel is de cyberrisico´s in de watersector helder te krijgen, de samenwerking te versterken, van elkaar te leren en daarmee de digitale weerbaarheid van de waterketens gezamenlijk te vergroten. Tegenover de kansen van digitalisering staan bedreigingen, bijvoorbeeld op het gebied van cybersecurity. Dit vraagt van de waterpartners om een gezamenlijke aanpak en inspanning.

3 TIPS

1. Weet met wie je samenwerkt en wie je ketenpartners zijn;
2. Blijf niet te lang aan de vergadertafel zitten;
3. De vertrouwelijkheid die om zaken heen hangt kan een goede samenwerking in de weg zitten.
   Wees daar alert op.

WOORDENBOEK HELPT OM ELKAAR BETER TE BEGRIJPEN

In de wereld van cybersecurity wordt zeer veel vakjargon gebruikt. De noodzaak om elkaars taal te spreken is bij cybersecurity van groot belang. De Cybersecurity Alliantie is een netwerk voor publiek-private partijen om samen te werken aan een digitaal weerbaar Nederland. Het project Cybersecurity Woordenboek draagt hieraan bij. Dit woordenboek, met ruim 600 cybersecuritytermen, slaat een brug tussen woorden die voor vakspecialisten gesneden koek zijn, maar voor afnemers van cybersecuritydiensten vaak onbekend. Op deze manier draagt het woordenboek bij aan een digitaal veilig Nederland. Als iedereen dezelfde taal spreekt, is het gemakkelijker om vraag en aanbod dichter bij elkaar te brengen en om een goede risico-inschatting te maken. Maar, zo is ook al duidelijk: het woordenboek moet constant bijgesteld worden. Het is nooit af.

'We zijn er trots op dat zowel gebruikers als aanbieders van cybersecuritydiensten samen hebben gezeten om de terminologie te verzamelen in één woordenboek.'

HACK_RIGHT LEIDT JONGE HACKERS NAAR HET RECHTE PAD

Jongeren die zich schuldig maken aan hacken realiseren zich vaak niet wat de gevolgen hiervan zijn en hoe groot de schade is. Speciaal voor jonge hackers tussen de 12 en 23 is 'Hack_Right' ontwikkeld; een alternatief, onderdeel of aanvulling op een strafrechtelijk traject. Het doel is om deze 'first offenders' op het rechte pad te krijgen én te houden. Hack_Right bestaat uit vier modules, die je kunt zien als vier puzzelstukjes: herstel, training, het bieden van een alternatief en coaching. Elke module voegt iets toe aan de gedragsverandering van de jongeren.

'Vaak hebben hackers niet door wat voor (ontwrichtende) schade hun acties teweeg brengen. Als we hen daarop wijzen hebben ze echt geen idee. Maar wat drijft ze dan? Als wij vragen 'Waarom heb je het gedaan?', wat denk je dat het antwoord is? 'Gewoon, omdat het kan!'

Floor Jansen, criminoloog en strategisch adviseur van het Team High Tech Crime van de Politie

'SPION OP JE PAD' TOETST KENNIS OVER INFORMATIEVEILIGHEID

Het bordspel 'Spion op je pad' is voor de ministeries van EZK en LNV ontwikkeld om de kennis van medewerkers over informatiebeveiliging te toetsen en te vergroten. In het spel maken de deelnemers kennis met dilemma's rondom informatiebeveiliging en privacy. De spelers moeten er samen voor zorgen dat de 'Spion' de waardevolle informatie die het team heeft, niet in zijn bezit krijgt. Zij werken onder tijdsdruk en moeten telkens de afweging maken tussen beveiliging, snelheid en kwaliteit.
Het is een dynamisch spel vol dilemma's. De deelnemers spelen niet tegen maar mét elkaar en testen zichzelf met vragen als: 'Je hebt een USB stick gevonden, wat doe je nu?'. Maar ook: 'Hoe gevoelig is de informatie waar ik mee werk, hoe ga ik ermee om en wat gebeurt er als gevoelige informatie op straat komt te liggen?'
In de toekomst wordt het spel nog verder aangepast. Zo worden er meer privacy-kwesties in de opgaven verwerkt.

HET NORMENKADER BIO KOMT ERAAN!

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. Deze vervangt de bestaande baselines informatieveiligheid van de verschillende bestuurslagen. De BIO is een doorontwikkeling, een update van de huidige BIG (Baseline Informatiebeveiliging Gemeenten). Hiermee ontstaat een eenduidige herkenbare stevige basis voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. De voorbereidingen op de implementatie van de BIO zijn momenteel in volle gang.

'Ik verdiep mij niet in Informatiebeveiliging omdat ik niets over ICT weet, is hetzelfde als: Ik verdiep mij niet in personeelsbeleid omdat ik niet weet hoe het lichaam werkt.'


OVERHEIDSBREDE
CYBEROEFENING
Wat zou jij doen?
ICTU

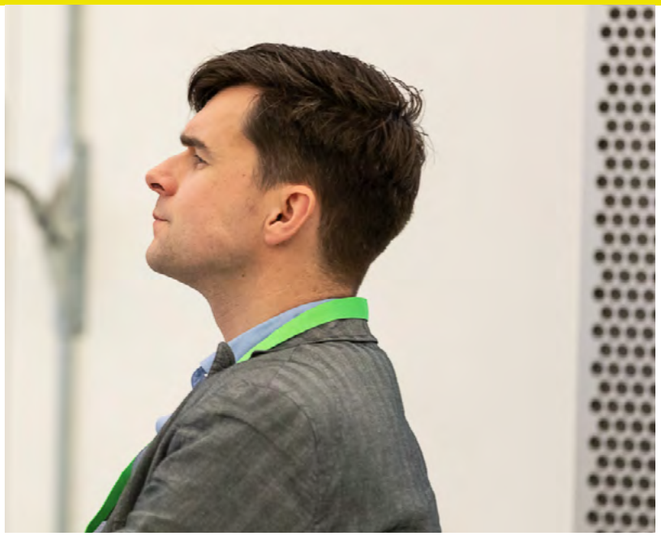

CIP
Agile Security Management


OVERHEIDSBREDE
CYBEROEFENING

WAT BEDREIGT DE GROTE STAD?

De gemeente Utrecht heeft met haar partners in kaart gebracht met welke dreigingen de stad te maken heeft. En dan vooral dreigingen toegespitst op cybercriminaliteit. Wie of wat kan het openbare leven in deze grote stad ontwrichten? En waar liggen de raakvlakken tussen de digitale en fysieke wereld? Lees hier de uitkomsten van het onderzoek.

'We moeten leren van problemen door de oplossingen met elkaar te delen.'



DE LESSEN VAN LEEUWARDEN

Het Digital Trust Center (DTC) werkt samen met partners binnen en buiten de overheid. In samenwerking met de VNG deed het DTC een eerste verkenning naar de rol van gemeenten om cyberweerbaarheid breder onder de aandacht te brengen. Het doel was om de succes-en faalfactoren in kaart te brengen die van belang zijn om ondernemers te helpen om cyberweerbaar te worden. Het onderzoek laat zien dat het belangrijk is om binnen gemeenten samen te werken aan veiligheid. Cyberveiligheid gaat immers verder dan de IT- of OOV (Openbare Orde en Veiligheid) afdeling.

'Het zou interessant zijn om te zien hoe de VNG hier een rol in kan spelen.'

De gemeente Leeuwarden is één van de gemeenten die mee heeft gewerkt aan deze verkenning. In Leeuwarden staat cyberveiligheid hoog op de agenda. Onlangs is daar een uitgebreide cyberoefening gehouden om de gemeente voor te bereiden op een cybercalamiteit. Dit zijn de lessons learned:

- Het is belangrijk om dezelfde 'taal' te spreken zodat medewerkers elkaar begrijpen en snel kunnen handelen wanneer een incident of crisis zich voordoet;
- Haal expertise aan tafel bij het gemeentelijk beleidsteam (GBT), zoals de CISO of CIO;
- Wie heeft het voorzitterschap binnen het gemeentelijk cyberteam (GCT)? Het is belangrijk dat goed vast te stellen;
- Om effectief te kunnen functioneren moet het GCT een vaste methodiek adopteren;
- Binnen het GCT worden veel technische/organisatorische beslissingen genomen, maar horen die hier eigenlijk wel thuis?

Een deelnemer na afloop van de sessie:

'Deze workshop liet duidelijk zien dat het noodzakelijk is om elkaar te kunnen vinden binnen een organisatie. Daarnaast werd het nogmaals duidelijk dat communicatie naar buiten toe een grote rol speelt en nog vaak wordt onderschat.'

VOORBEREIDEN OP DIGITALE ONTWRICHTING

Digitale infrastructuur – is vaak zonder dat we het merken – intens verweven met processen die van groot belang zijn voor de samenleving, de economie en de democratische rechtstaat. Voor verstoringen in de fysieke wereld bestaan professionele crisisorganisaties en uitgebreide wet- en regelgeving. De voorbereiding op een digitale ontwrichting krijgt echter nauwelijks tot geen aandacht. In het rapport 'Voorbereiden op digitale ontwrichting' pleit de WRR voor een goede voorbereiding door o.a. adequate bevoegdheden om escalatie te voorkomen en inspanningen op het terrein van cyberverzekeringen te verrichten.

'De uitdagingen zitten in de verwevenheid van fysiek en digitaal. Fysiek is er al veel meer vastgelegd qua regelingen en wetten, digitaal staat dat nog in de kinderschoenen.'

SCHOOL, TBS-KLINIEK OF FAKE NEWS?

Deelnemers aan de game 'School, tbs-kliniek of fake news' kropen in de rol van een crisisteam. Hen werd gevraagd met een oplossing te komen tijdens een digitaal incident dat flink uit de hand dreigt te lopen.

Bij de balie van een gemeente melden zich verontruste burgers. Zij hebben op de website van de gemeente gelezen dat de bouw van een basisschool niet doorgaat. In plaats daarvan komt er nu een half open tbs-kliniek. In beroep gaan heeft geen zin. Het gemeentelijk callcenter is bovendien onbereikbaar. Het bericht is nep, de verantwoordelijk wethouder vraagt om hulp. Het verwijderen van het bericht blijkt niet eenvoudig. Niemand kan meer inloggen in het CMS. Het callcenter heeft ondertussen al uren geen telefoontjes meer ontvangen. Het crisisteam krijgt de vraag voorgelegd één en ander in goede banen te leiden. De gemeenteraadsvergadering van later die dag mag geen chaos worden.

Steeds sneller fysiek

Deelnemers vonden de game 'een geweldige manier om zaken bespreekbaar te maken'. Belangrijke les: digitale incidenten worden steeds sneller fysiek. Wat gebeurt er bijvoorbeeld als de OV-chipkaart een paar achtereen gesloten dagen niet werkt? Of als de 112-noodlijn er even uit ligt? De conclusie van een van de deelnemers: "We moeten veel meer samenwerken met IT."

IN DE ESCAPE ROOM

Je team staat aan de rand van een grote doorbraak met een bepaalde technologie. Na jaren hard werken zijn jullie bezig met de puntjes op de 'i'. Als jullie uitvinding een succes wordt zijn jullie zonder twijfel allemaal miljonair. Er is alleen een probleem: er is een groot datalek in het systeem gevonden waar jullie onderzoek in is opgeslagen. Aan jullie de taak om te voorkomen dat het onderzoek uitlekt.

Social hacking, privacy en cybersecurity zijn centrale thema's in deze uitdagende escaperoom van Alert Online. Een aantal deelnemers van de overheidsbrede Cyberoefening ging de uitdaging aan. Wat hebben zij geleerd?

'Let op wat je online doet en wat voor gegevens je online invult, aangezien hackers er makkelijk bij kunnen. In één seconde kan een computersysteem twee miljard wachtwoorden uitproberen. Je bent ontzettend snel je gegevens kwijt.'

'Het was een leuke, creatieve en interactieve manier om je bewustzijn te verhogen, met situaties die je ook in het dagelijkse leven tegenkomt!'

BESTUURLIJKE DILEMMA'S BIJ CYBERGEVOLGBESTRIJDING

Op bestuurlijk niveau is een goede cybergevolgbestrijding van groot belang. De cyberoefening levert hier een grote bijdrage aan. Tegen welke dilemma's lopen bestuurders aan als het zover komt? En wat is een crisis met een cybercomponent eigenlijk? Welke rol wordt dan van de bestuurders verwacht?
Het COT instituut voor Veiligheids- en Crisismanagement adviseert en verzorgt trainingen. Marco Zanoni (COT): "Jouw cybersecurity moet vóór een crisis al inzichtelijk en uitgewerkt zijn". En: "Als de veiligheid in het geding is, is de rest relatief".

Lessons learned

- Identificeer op voorhand al wat de voorspelbare (crisis) momenten zijn en welke besluiten er dan genomen moeten worden;
- Focus bij een cybercrisis niet op aannames en scenario's maar op de feiten;
- Weet wat de kroonjuwelen zijn die je wilt beschermen.

NATIONAAL CRISISPLAN-ICT ONDERSTEUNT BIJ CYBERINCIDENT

ICT is niet meer weg te denken uit onze hedendaagse samenleving, vrijwel alle vitale processen zijn hiervan direct afhankelijk. ICT kwetsbaarheid kan leiden tot een verstoring of uitval van (vitale) processen in de samenleving.
Om een dergelijke situatie te beheersen is het Nationaal Crisisplan ICT (NCP-ICT) opgesteld. Het NCP-ICT is een specificering van de generieke crisisstructuur zoals beschreven in het Nationaal Handboek Crisisbesluitvorming.

Lessons learned

- Een belangrijke vraag is: wat heeft een aanval op de ene sector voor effect op een andere sector? Hier moet rekening mee worden gehouden bij het maken van een crisisplan;
- Cybergevolgbestrijding = crisisbeheersing. Hierbij is het uitgangspunt: bestaande structuren, rollen en werkwijzen, maar heb ook oog voor het afwijkende;
- We proberen te leren van de incidenten die reeds hebben plaatsgevonden;
- Cybermensen moeten meer de taal van de crisisbeheersing spreken. En de crisisbeheersing moet meer weten over Cybertaal;
- We zijn nog in ontwikkeling op het gebied van Cyber, maar gooi multidisciplinaire crisisbeheersing niet overboord.

DE ACTUELE DREIGING VAN IoT

Organisaties raken steeds meer verweven met technologie en technische toepassingen. De ontwikkelingen gaan razendsnel. Het is van groot belang dat de verschillende organisaties zich beschermen tegen de toenemende cyberdreigingen van Internet of Things (IoT).

Kwetsbaarheden in IoT apparaten en -systemen kunnen de impact van cyberaanvallen vergroten. Organisaties moeten daarom zo vroeg mogelijk in staat worden gesteld om IoT-hacks, malware besmettingen en andere cyberaanvallen vroegtijdig te herkennen en te voorkomen.
Neem het recente voorbeeld van Mirai-botnet*. Dat bestond uit IoT-apparaten die slecht beveiligd waren en daardoor werden gehackt. Die apparaten werden vervolgens ingezet om websites neer te halen door middel van een DDoS-aanval**. Een voorbeeld dat de urgentie toont, stelt Ben van Lier, directeur Strategie en Innovatie van Centric.

Lessons learned

- 'Er is een ecosysteem van apparaten ontstaan';
- 'Systemen worden steeds autonomer, waardoor we er dus ook minder over te vertellen hebben. Tegelijkertijd willen we ook steeds meer aan de systemen overlaten';
- 'We creëren iets waarvan we de gevolgen eigenlijk niet kunnen overzien.'

* De Mirai-malware verscheen in 2016 en wist allerlei Internet of Things-apparaten te infecteren. Op het hoogtepunt bestond het uit honderdduizenden apparaten, aldus het Amerikaanse openbaar ministerie.

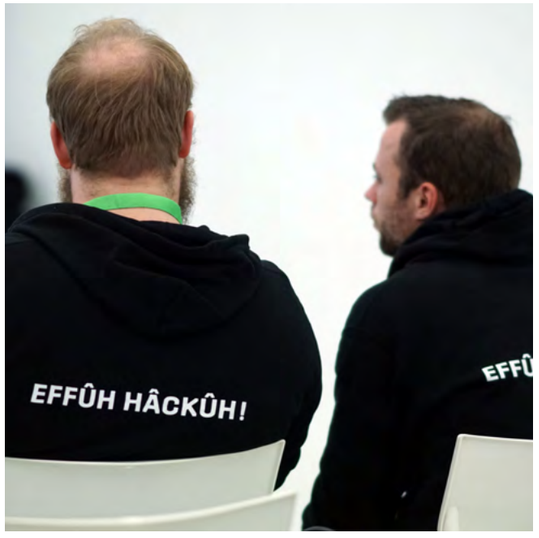
** Bij een DDoS-aanval (Distributed Denial of Service) worden er vanuit een netwerk van computers in een keer heel veel data naar een server gestuurd, veel meer dan normaal gesproken. Door deze vloedgolf aan informatie zijn de servers tijdelijk offline óf slecht bereikbaar.

BESTRIJD EEN HACK MET DE CIP CRISIS GAME

De CIP Crisis Game is een teamspel waarin deelnemers werken voor een fictieve organisatie die wordt gehackt en wordt afgeperst.

De deelnemers staan voor de taak deze hack zo efficiënt mogelijk te bestrijden, te voorkomen dat de data bij onbevoegden terecht komt, en te achterhalen wie de dader is. Tijdens deze crisisgame doen zich, net als in de praktijk, meerdere nieuwe situaties voor waarop zo goed mogelijk moet worden ingespeeld om de schade te beperken.
Tijdens de game kregen de deelnemers, verdeeld in vijf teams – Crisiscoördinatie, Privacy, Communicatie, SOC (Security Operations Centre) en Business management – een keuzelijst met acties die ze konden ondernemen. De volgorde van deze acties was zeer bepalend voor het spelverloop. Opdracht: voorkomen dat de hacker ervandoor gaat.

‘HACK DEN HAAG’ TEST CYBERSECURITY



Alle organisaties, waaronder gemeenten, staan dagelijks bloot aan digitale dreigingen als phishing en hackpogingen. Optimale digitale veiligheid is dan ook cruciaal.

In het kader van de ‘transparante overheid’ laat de gemeente Den Haag jaarlijks de ICT-systemen van de stad en de leveranciers testen op kwetsbaarheden. Dit gebeurt door professionele hackers, tijdens de hacking game ‘Hâck The Hague’. Op deze manier wordt samen met de hackers de veiligheid van de stad verbeterd.

Lessons learned

- Tijdens ‘Hâck The Hague 2019’ werden 200 kwetsbaarheden gevonden;
- Hackers hebben tijdens dit evenement meer opties om binnen te dringen, maar ook veel minder tijd dan tijdens een pentest. Echter zijn er veel meer deelnemers, waardoor er ook veel meer kan worden uitgeprobeerd;
- Het bestaande *responsible disclosurebeleid* is gebruikt als basis voor de *rules of engagement*;
- Veel kwetsbaarheden worden razendsnel wereldwijd *gepatcht*. Er werd zelfs een keer al tijdens de *challenge gepatcht*;
- Het is slim om gebruik te maken van de kennis van de hackercommunity;
- Beloningen sturen aan mensen die een lek vinden? Het is belangrijk dan wel kaders te stellen aan *bug bounty* programma’s. Anders word je constant bestookt door mensen die met kleinigheden een vergoeding proberen te krijgen.

NEVER WASTE A GOOD CRISIS

Op verschillende manieren lopen lokale overheden risico’s in het informatiebeveiligingsdomein. Van knullige fouten tot uiterst geraffineerde vormen van digitale fraude: de gevolgen zijn vaak groot als het misgaat. Bewustwordingscampagnes zijn veelal gebaseerd op situaties waar de doelgroep zich niet of nauwelijks mee kan identificeren. Maar door de voorbeelden in deze campagnes dichter bij de praktijk te brengen wordt de impact groter, denkt Geert Schoots (CISO Gelderland). “Van fouten kun je namelijk altijd leren, vooral als ze herkenbaar zijn.”

Geert had een aantal opmerkelijke voorbeelden bij zich. Zoals twee op het oog onschuldige foto’s: eentje van een setting binnen en de andere van een setting buiten. Echter, door in te zoomen was in beide gevallen vertrouwelijke informatie te vinden. Via een open deur, door een raam....

Lessons learned

- Je organisatie is groter dan je denkt. Elke thuiswerkplek is ook een werklocatie, dus veel organisaties hebben wel duizend werkplekken.
- Het is erg belangrijk om in je organisatie een sfeer te creëren waar fouten die gemaakt zijn ook veilig gedeeld kunnen worden.

INFORMATIEVEILIGHEIDSLADDER: INSTRUMENT VOOR BEWUSTZIJN

Bestuurders en managers vervullen een belangrijke rol in het tot stand brengen van een informatieveiligheidscultuur. Het is confronterend om te merken hoe gemakkelijk je om de tuin kan worden geleid en iets doet wat achteraf gezien een inbreuk op de informatieveiligheid heeft. Had dat voorkomen kunnen worden? Na bezinning volgt ambitie: Wat willen of moeten we hier tegen doen? Dan is het tijd voor actie: Hoe gaan we dat doen? Dan reflectie: Hoe gaan we in de toekomst met onze rol om? De Informatieveiligheidsladder van Provincie Fryslan kan hierbij helpen.

Lessons learned

- Bepaal je informatieveiligheidsklimaat, analyseer de uitkomst, ga in gesprek op de werkvloer (waarom doen we dingen zoals we die doen). Bepaal verbeterpunten, wees actiebereid en investeer in mensen;
- Als je geen leiderschap en betrokkenheid van jouw bestuur meekrijgt, dan ga je nooit op een hogere trede komen op de veiligheidsladder.

TELEKWETSBAARHEID HELPT BIJ UITVAL

Telecommunicatie is nodig. Voor het maken van reisdocumenten tot het functioneren van de riolering. En van de gehele kantoorautomatisering tot aan het monitoren van pompen en gemalen. Maar hoe vanzelfsprekend is de beschikbaarheid van telecommunicatie eigenlijk?

Een cyberaanval, een kabel die geraakt wordt bij graafwerkzaamheden, een update die verkeerd uitpakt; uitval is nooit helemaal te voorkomen en de impact kan groot zijn. Het programma Telekwetsbaarheid van Agentschap Telecom helpt organisaties maatregelen te treffen tegen de gevolgen van telecomuitval. Met praktische instrumenten als een vijfstappenplan en checklists ontdekken organisaties waar de risico’s van telecomuitval liggen en de manieren waarop ze deze kunnen beperken.

‘Eigen verantwoordelijkheid is van belang; de I in ICT is van Iedereen.’

Dit zijn de vijf stappen

1. Bewustwording
2. Afhankelijkheden in kaart brengen
3. Risico’s benoemen
4. Maatregelen treffen
5. Fit blijven als organisatie

OVERHEIDSBREDE CYBEROEFENING

WAT ZOU JIJ DOEN?

WHY?

VEEL AANDACHT AL VOOR AWARENESS, MAAR WAT ALS ER ÉCHT IETS GEBEURD? → OEFENEN! —BE PREPARED!—

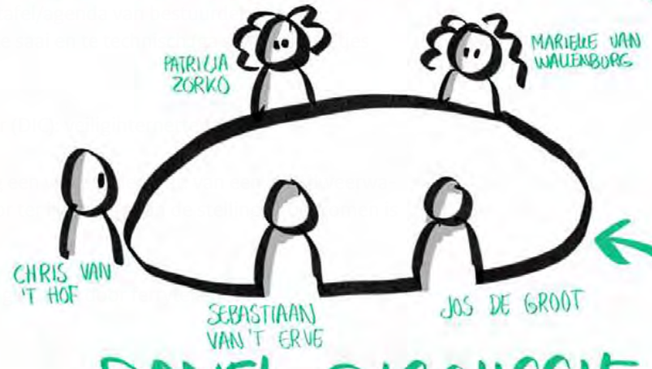
RAYMOND KNOPS
STAATSSECRETARIS MIN BZK

CYBER-DREIGING VAAK NIET ZICHTBAAR = GEEN PROBLEEM?!

"DE VRAAG IS NIET ÓF, MAAR WANNEER EN HOE GROOT EEN CYBER-ATTACK PLAATSVINDT!"

- PREVENTIE, DAAR BEGINT HET MEE! → BIO
- BEVEILIGINGSNIVEAU OVERHEID IS AL BETER!

MAAR BLIJF KENNIS, UIT PRAKTIJK MET ELKAAR DELEN!



PANEL-DISCUSSIE

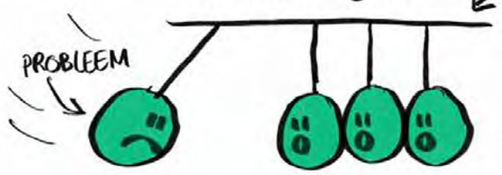
GROOTSTE DREIGINGEN:

* "CYBER-CRIMINALITEIT"
* SPIONAGE DOOR ANDERE STATEN

DIGINOTAR

2017 ROTTERDAMSE HAVEN

LESSONS LEARNED:
ALLES IN SYSTEEM AAN ELKAAR GEKNOOPT
"KETENS AFHANKELIJKHEID"



WE ZIJN ALS MENSEN STEEDS AFHANKELIJKER VAN **CONTINUÏTEIT** VAN DE SYSTEMEN & "INTERNET OF THINGS"
↳ WEERBAARHEID & BACK UPS ZEER BELANGRIJK!

KOMENDE TIJD AANDACHT VOOR:

UPDATES

VEILIGE HARD- & SOFTWARE
INCL. "CERTIFICERING"

OVERHEDEN MOETEN DE PUBLIEKE WAARDE BESCHERMEN!
CASUS ROTTERDAM: REKENKAMER RAPPORTEERDE 2.000 KWETSBAARHEDEN.
ONDERWERP MOET OP TAFEL/AGENDA BESTUURDERS!

VOORKOMEN IS VÉÉL BETER DAN GENEZEN

DE DIGITALE BRANDWEER
ALS METAFOOR

2019 LOCHEM

RANSOM-WARE GEMEENTE LOCHEM: GELIJK OPGESCHAALD NAAR EEN "CRISIS"!
1 COMMUNICATIE HEEL BELANGRIJK!
2 ONDERZOEK DOEN NAAR DADERS (BELASTBARE FEITEN)
3 HELE ICT-SYSTEEM OPNIEUW MOETEN OPBOUWEN! → IN 1 DAG!
* STANDAARDISATIE VAN IT-LANDSCHAP WAS SUCCES-FACTOR
* BIJ LOCHEM WAS HET OVER-ZICHTELIJK: 1 GEBOUW
↳ WEL 200 KOPPEL-VLAKKEN MET ANDERE ORGANISATIES.
"OOK MET 112 VIA DE VEILIGHEIDSREGIO"

"AANVAL OP 'DE ÉÉN', IS EEN AANVAL OP 'DE ANDER'..."
↳ NET ALS DE BANKEN!

TIP DIGITAL TRUST CENTER (DTC)
↳ VEILIGINTERNETTEN.NL

MAAK PREVENTIE NIET TE SAAI & TE TECHNISCH!
SAMEN "SPELLETJES SPELEN"!

FEDDY TEKENT.NL

LESSONS LEARNED

Cybersecurity is een lastig onderwerp en vaak een technisch verhaal, stelt Chris van 't Hof, moderator tijdens de overheidsbrede cyberoefening 'Wat zou jij doen?' 'Nu we geoefend hebben voelen we het in de onderbuik en gaat het leven. De kunst is nu om er iets mee te gaan doen, want *never waste a good crisis.* En als er wat gebeurt, wat kunnen we dan doen om herhaling te voorkomen? Leren van elkaar, erkennen dat er een onderlinge afhankelijkheid is en samen werken aan een concreet handelingsperspectief: dat is de opdracht voor de toekomst.' Waarbij we volgens Van 't Hof de volgende lessen in acht moeten nemen:

- Blijf oefenen!
- Het begint met preventie
- De keten is groot, we zijn van elkaar afhankelijk
- Werk met veilig en goed materiaal en zorg voor updates
- Deel cyberkennis met elkaar
- Zorg dat je weerbaar en wendbaar bent
- Als het fout gaat: trek je les en voorkom herhaling

MEER INFORMATIE?

BEKIJK DE TOOLBOX OP

DIGITALEOVERHEID.NL/TOOLBOX-CYBERINCIDENT

OF BEZOEK WEERBAREDIGITALEOVERHEID.NL