Zie voor laatste CIP-cast: http://beveiligingsupdate.nl/

CIP-CAST PORTFOLIO

Klik in de inhoudspagina om

direct naar de CIP-Cast van uw keuze te gaan.

Inhoud

Inleiding

CIP stelt korte filmpjes beschikbaar die door iedereen ingezet kunnen worden om de informatieveiligheid te verhogen. De filmpjes duren in het algemeen maximaal 5 minuten. Deze filmpjes noemen we CIP-Casts.
De filmpjes bevatten veelal interviews waarin maatregelen tegen dreigingen worden besproken.
Onderstaand vind je op onderwerp een toelichting op de CIP-Casts. Met deze onderverdeling kun je makkelijk zoeken of er een voor jou geschikte CIP-Cast tussen zit.
Bovendien kan er makkelijk doorgeklikt worden naar de betreffende CIP-Cast.
Bij iedere CIP-Cast is kort aangegeven wat de inhoud van de CIP-Cast is, voor welke doelgroep deze primair bedoeld is en welke leerpunten je eruit zou kunnen halen.
Aan de datum kun je zien wanneer deze CIP-Cast gepost is.

1. E-Mail

1.1. Nepmails van de bank en Phishing

2-7-2015
Doelgroep:
Iedereen die e-mail gebruikt.

Beschrijving
Een van de populairste vormen van internetcriminaliteit is phishing. Dat zijn trucs om gegevens van mensen in handen te krijgen door bijvoorbeeld een e-mail te sturen namens een bank of andere organisatie. Meestal is het verzoek om informatie te geven. Op het moment dat u op links van dit soort berichten klikt, komt u vaak op de website van criminelen uit. Alleen het bezoek is vaak al voldoende om uw computer te infecteren. Ook is het kinderlijk eenvoudig om inloggegevens over te nemen. Hoe simpel dat is legt beveiligingsexpert Wouter Slotboom aan Ad Reuijl van het CIP uit. Ook demonstreert hij hoe eenvoudig het is voor criminelen om misbruik te maken door een bestaande website te kopiëren en ingevoerde gegevens te achterhalen.

Leerpunten
- Een bank zal nooit een e-mail sturen waarin ze vragen om login-gegevens of andere informatie. Lees de zes tips van Veilig Internetten om gewapend te zijn tegen nepmails of nep telefoontjes;
- Klik niet op links naar login-pagina's. Een bank zou dat niet doen;
- Voer zelf het adres van uw bank in de webbrowser in als u wilt gaan internetbankieren;
- Leer nepmails herkennen;

Lees ook de tips op veilig interentbankieren van de banken om phishing-ellende te voorkomen.

Directe link
https://beveiligingsupdate.nl/2015/07/02/wouter-slotboom-over-nepmails-van-de-bank-en-phishing/

1.2. Test met Phishing mail binnen een organisatie

16-7-2015
Doelgroep
Iedereen die e-mail gebruikt, medewerkers die een phishing campagne willen opzetten.

Beschrijving
Hoe simpel is het nu om een awareness-campagne op te zetten? Studenten van de Hogeschool van Rotterdam onderzochten dat door hun hun eigen medestudenten te bestoken met een phishing-mail. Uiteraard was er eerst toestemming gevraagd. De studenten deden dat in het kader van 'Privacy Lab', een opdracht waar verschillende opleidingen met elkaar samenwerken. Harin Indira Familia Turbi en Thierry Karsemeijer, twee projectdeelnemers, vertellen Ad Reuijl, directeur van het CIP, hoe ze te werk gingen, hoeveel mensen er daadwerkelijk in trapten en hoe simpel het is om mensen te misleiden.

Leerpunten
- Op veiliginternetten.nl staat beschreven hoe een phishing-mail te herkennen is;
- Bent u er toch in getrapt en vreest u slachtoffer te zijn dan staan hier diverse goede tips;
- Ook de banken hebben de nodige tips om phishing tegen te gaan;
- Krijgt u op kantoor een phishing-mail? Meldt het dan bij uw IT-afdeling of systeembeheerder;
- Waar moet je rekening mee houden als je een phishing-campagne opzet;
- Vraag altijd eerst toestemming voordat je en phishing-actie opzet.

Directe link
https://beveiligingsupdate.nl/2015/07/16/studenten-bestoken-eigen-school-met-phishing-mail/

1.3. Veiliger versturen van e-mail

14-8-2015
Doelgroep
Iedereen die meer wil weten over het belang van e-mail encryptie.

Beschrijving
Als je een e-mailbericht stuurt. Hoe veilig is dat eigenlijk? Vaak voelt dat vertrouwt aan. Maar kunnen andere partijen meelezen met onze berichten? En als dat kan wat kunnen we daartegen doen? Beveiligingsexpert Hans de Raad van OpenNovations praat daarover met Ad Reuijl van het CIP.

Leerpunten
Je moet e-mail encrypten, zodat anderen niet ongewenst mee kunnen lezen.

Directe link
https://beveiligingsupdate.nl/2015/08/14/hans-de-raad-over-het-veiliger-versturen-van-e-mail/

1.4. Omgaan met phishing

30-10-2016
Doelgroep
Iedereen die e-mail van buiten het eigen netwerk ontvangt.

Beschrijving
Nog altijd schort het aan bewustzijn over phishing. De kwalijke berichten worden nog massaal aangeklikt als ze goed genoeg zijn opgesteld. Dat ontdekten Hans Labruyere en Marciano Kruithof van LBVD bij hun onderzoek naar het bewustzijn. Zij pleiten voor een cultuurverandering en anders kijken naar de problematiek.

Leerpunten
- Oefen met phishing-acties;
- Om informatieveiligheid te verhogen, is een cultuurverandering nodig;
- Informatieveiligheid moet van "moeten" naar " willen": als je het belang van informatieveiligheid aan je medewerkers kunt uitleggen, dan zal de wil ontstaan om mee te werken.

Directie link
https://beveiligingsupdate.nl/2016/10/30/hans-labruyere-en-marciano-kruithof-over-omgaan-met-phishing/

1.5. Veilig e-mailgebruik

6-4-2016
Doelgroep
Iedereen die privé e-mail via zijn of haar zakelijke e-mailaccount verstuurd vice versa.

Beschrijving

Tijd en plaats onafhankelijk werken leidt ertoe dat medewerkers hun werk e-mailadres ook voor privé doeleinden gebruikt en ook privé e-mail voor zakelijk gebruik. Is dit altijd schadelijk? Wat kan een werkgever doen om de werknemer te informeren over de do's en don'ts van e-mailgebruik? Beveiligingsexpert Hans de Raad spreekt hierover met Jan Renshof van het CIP.

Leerpunten
- Gebruik een server onder eigen of vertrouwd beheer en niet een openbare cloudserver;
- Een e-mail is qua openbaarheid vergelijkbaar met een briefkaart;
- Maak gebruik van versleuteling.

Directie link
https://beveiligingsupdate.nl/2017/04/06/hans-de-raad-over-veilig-e-mailgebruik/

2. Datalekken

2.1. Meldpunt datalekken

30-7-2015
Doelgroep
Medewerkers die verantwoordelijk zijn voor de gegevenshuishouding.

Beschrijving
Wie persoonsgegevens verwerkt moet dat zorgvuldig doen en voor de beveiliging zorg dragen. Gaat het mis dan moeten incidenten vanaf 1 januari 2016 gemeld worden. Wordt de wet overtreden dan riskeren organisaties forse boetes. Niet alleen voor het niet melden zijn boetes mogelijk, maar ook voor het niet op orde hebben van de beveiliging. Wat dit allemaal betekent legt Sergej Katus van Privacy Management Partners uit aan Elleke Oosterwijk van het CIP.

Leerpunten
- Leer wat de meldplicht datalekken inhoudt;
- Wat moet je doen als je een datalek hebt;
- Wat moet je doen om te voorkomen dat er een datalek ontstaat;
- Organiseer een procedure om datalekken te detecteren;
- Denk na over een veilige informatiehuishouding, je privacy management: hoe ga je om met gegevens van mensen.

Directe link
https://beveiligingsupdate.nl/2015/07/30/sergej-katus-de-aankomende-meldplicht-datalekken/

2.2. Ik heb een datalek. Wat nu?

18-2-2016
Doelgroep
Medewerkers die verantwoordelijk zijn voor de gegevenshuishouding.

Beschrijving
Sinds 1 januari 2016 geldt er een meldpunt datalekken voor alle organisaties in Nederland. Iedere organisatie moet datalekken melden aan de Autoriteit Persoonsgegevens. De vraag is hoe je erachter komt dat jouw organisatie een datalek heeft. Erik de Jong van Fox-IT legt aan Brenno de Winter uit hoe je datalekken kunt opsporen en wat je moet vastleggen om bij misdaad eventuele daders te identificeren.

Leerpunten
- Welke stappen moet je ondernemen als een datalek ontdekt is;

- Welke vragen moet je stellen als een datalek ontdekt is;
- Welke governance moet je binnen je crisisteam inregelen;
- Inrichten van logging en monitoring om een datalek sneller te detecteren.

Directe link
https://beveiligingsupdate.nl/2016/02/18/erik-de-jong-ik-heb-een-datalek-wat-nu/

2.3. Voorbereiden op een datalek

18-3-2017
Doelgroep
Bestuurders en medewerkers van crisisteams die ingezet worden wanneer een datalek een feit is.

Beschrijving
Iedere organisatie wordt een keer geconfronteerd met een datalek. Met die wetenschap kun je voorbereidingen treffen om de gevolgen te beperken als de situatie zich opeens aandient. Welke plannen moet je maken en hoe reageer je als er echt een datalek is. Remco Groet van de Informatiebeveiligingsdienst (IBD) gaat in gesprek met Brenno de Winter over het voorbereiden en het omgaan met een datalek.

Leerpunten
- Denk na over een datalek **voordat** het optreedt;
- Wees transparant;
- Oefen een datalek regelmatig en zorg dat iedereen elkaar kent;
- Maak een goed communicatieplan: zie factsheet op de website van IBD met communicatietips.

Directe link
https://beveiligingsupdate.nl/2017/03/18/remco-groet-voorbereiden-op-een-datalek/

2.4. Wie helpt nu met wat bij informatiebeveiliging?

20-4-2017
Doelgroep
Medewerker informatiebeveiliging, crisisteams informatiebeveiliging

Beschrijving
Het Nationale Cyber Security Centrum (NCSC) en de Informatiebeveiligingsdienst (IBD) helpen organisaties wanneer een incident rond informatiebeveiliging optreedt. Maar wie nu doet nu wat en wat mag je van welke oganisatie? NCSC richt zich daarbij primair op het Rijk en de vitale sectoren en IBD op de gemeenten. Zij kunnen organisatie helpen bij het melden van incidenten maar ook in de juiste richting wijzen bij het afhandelen van een incident. Maar voorkomen is beter dan genezen daarom bieden ze baselines aan om de basis op orde te hebben en zo preventief maatregelen te nemen ter bescherming. Martijn Hamer van het NCSC en Nausikaa Efstratiades van de IBD vertellen aan Elleke Oosterwijk wat we van hun organisaties nu wel en vooral wat we niet mogen verwachten.

Leerpunten
- NCSC en IBD hebben een coördinerende taak
- De organisaties richten zich vooral op de overheid (het NCSC ook op vitale sectoren)
- Organisaties blijven zelf verantwoordelijk voor de afhandeling van een incident
- Zet de BIG of BIR in om de basis op orde te hebben

Directe link
https://beveiligingsupdate.nl/2017/04/24/wie-helpt-nu-met-wat-bij-informatiebeveiliging/

3. Gegevens

3.1. Encryptie of versleuteling

18-6-2015
Doelgroep
Informatiebeveiliging specialisten.

Beschrijving
Wat is encryptie/versleuteling. Hoe werkt het. en In het beveiligen van onze omgeving hoor ik steeds vaker mensen praten over encryptie of versleuteling. Wat is dat nou? Waarom hebben we dat nodig? Wat betekenen termen als symmetrische versleuteling, asymmetrische versleuteling, PGP en S/MIME nou? Hans de Raad van OpenNovations is goed in staat dat simpel uit te leggen aan Ad Reuijl van het CIP.

Leerpunten
- Wat is encryptie/versleuteling;
- Hoe werkt het;
- Wat is het verschil tussen symmetrische en assymetrische versleuteling;
- Hoe S/MIME en PGP jouw e-mail versleutelt.

Directe link
https://beveiligingsupdate.nl/2015/06/18/hans-de-raad-over-encryptie-of-versleuteling/

3.2. Als je data op straat ligt

16-10-2015
Doelgroep
Informatiebeveiliging specialisten.

Beschrijving
Wat betekent het nou als je data op straat ligt? Wat gebeurt er met onze gegevens als ze in de handen van criminelen vallen. Welke stappen kun je zitten om de risico's te beperken dat als een website gehacked is je niet direct het slachtoffer wordt van identiteitsdiefstal? Tom de Haan, bezig met beveiliging bij het UWV praat erover met Meine van Essen van het CIP.

Leerpunten
- Wat betekent het als een database op straat ligt;
- Hoe werk SQL injection;
- Hoe kun je je beter beschermen met 2 factor authenticatie.

Directe link
https://beveiligingsupdate.nl/2015/10/16/tom-de-haan-als-je-data-op-straat-ligt/

3.3. Voorwaarden om persoonsgegevens te verwerken

3-12-2016
Doelgroep
Bewerkers van persoonsgegevens.

Beschrijving
Een organisatie die persoonsgegevens wil verwerken moet zich aan een aantal regels houden. We horen vaak dat we vooraf over zaken moeten nadenken. Maar dat is zo algemeen en niet helder als vanaf 1 januari 2016 er boetes kunnen worden uitgedeeld. Wat zijn de belangrijkste dingen waar je nu op letten en wat betekent dat voor organisaties? Advocaat Ot van Daalen praat daarover met Brenno de Winter.

Leerpunten
- Je bent gebonden aan de Wbp als je persoonsgegevens verwerkt;
- Wat is proportionaliteit, hieraan moet je voldoen;
- Je moet transparant zijn naar de mensen van wie je gegevens bewerkt;
- Je mag alleen gegevens gebruiken voor het doel waarvoor je ze verzameld hebt, doelbinding.

Directe link
https://beveiligingsupdate.nl/2015/12/03/ot-van-daalen-de-belangrijkste-voorwaarden-om-persoonsgegevens-te-verwerken/

3.4. Bewaren van gegevens

18-12-2016
Doelgroep
Beheerders van data.

Beschrijving
Persoonsgegevens mogen niet langer dan noodzakelijk worden bewaard. Maar nergens is beschreven hoe lang je dan gegevens mag bewaren. Ook het woord noodzakelijk is een nogal rekbaar begrip. Organisaties die niet goed met deze gegevens omgaan riskeren wel een boete. Hoe kun je het dan nog goed doen? Ot van Daalen, advocaat privacy-recht, legt uit hoe organisaties hier ondanks de onduidelijkheid toch tot een beredeneerde beslissing kan komen waar de toezichthouder mee uit de voeten kan.

Leerpunten
- Als er geen richtsnoeren zijn, kun je zelf onderbouwen hoe lang je gegevens kunt bewaren. Dit moet wel gedocumenteerd worden om aan te kunnen tonen dat er goed over nagedacht is;
- Privacy gevoelige gegevens moeten op een afgeschermde omgeving staan;
- Hoe moet je "conform de stand der techniek" interpreteren.

Directe link
https://beveiligingsupdate.nl/2015/12/18/ot-van-daalen-gegevens-niet-langer-bewaren-dan-noodzakelijk/

3.5. Hoe om te gaan met een Cryptolocker

17-3-2016
Doelgroep
Beheerders van data.

Beschrijving
Wat moet er gebeuren als je organisatie geconfronteerd wordt met een datalek. Natuurlijk is het eerst achterhalen wat er gebeurd is en wat de acties zouden moeten zijn. Maar hoe moet het forensisch onderzoek plaatsvinden, hoe moet je een crisis team inrichten, welke expertise moet daarin vertegenwoordigd zijn. Erik de Jong van Fox-it legt aan Brenno de Winter uit welke stappen een organisatie moet nemen om te achterhalen of er een datalek is en hoe daar mee om te gaan. Stel je hebt last van een cryptolocker wat kun je dan doen? Moet je ingaan op de eisen van de aanvallers en geld betalen? Hoe werkt het proces dan, als je ingaat op de chantage eisen hoe gaat dat dan?

Leerpunten
- Wat is een aanpak als er een incident heeft plaatsgevonden en forensisch onderzoek gestart moet worden;

- Maak altijd regelmatig back ups van je bestanden;
- Houd je systemen up to date;
- Wat is de business case van de crimineel die de cryptolocker inzet.

Directe link
https://beveiligingsupdate.nl/2016/03/17/erik-de-jong-hoe-moet-je-omgaan-met-cryptolocker/

3.6. Classificeren van gegevens

19-9-2016
Doelgroep
Beheerder van data.

Beschrijving
Niet alle gegevens zijn even belangrijk. Sommige mogen prima openbaar zijn, terwijl andere echt vertrouwelijk moeten blijven. Het onderscheid maken noemen we classificeren of met een mooi woord rubricering. Welke gegevens voorzie je van een hoog beveiligingsniveau en welke beveilig je minder of niet, een vraag waar organisaties mee worstelen. Hoe ga je om met kwetsbare informatie die niet in verkeerde handen mag vallen. Erik Stoops van het Openbaar Ministerie legt aan Elleke Oosterwijk van het CIP uit hoe rubricering van gegevens hiervoor kan worden ingezet.

Leerpunten
- Wees je bewust van welke informatie kwetsbaar is;
- Medewerkers moeten weten hoe kwetsbaar de gegevens zijn waarmee zij werken;
- Medewerkers moeten weten welke informatie beschermingsmaatregelen van toepassing zijn.

Directe link
https://beveiligingsupdate.nl/2016/09/19/erik-stoops-over-het-classificeren-van-gegevens/

3.7. Economische spionage

29-9-2016
Doelgroep
Medewerkers verantwoordelijk voor bescherming van de bedrijfsdata.

Beschrijving
Economische spionage is dit een risico, wat is het risico en kun je er iets tegen doen. Is er tooling beschikbaar om je hiertegen te beschermen en welke afwegingen moet je maken. Maarten van Wieren van Deloitte is gespecialiseerd op dit onderwerp en vertelt hierover.

Leerpunten
- Bepaal wat de waarde van je data;
- De wet beschermt je niet tegen (economische) spionage;
- Installeer altijd de laatste updates en patches;
- Monitor het verkeer op je netwerk, bv met advanced analytics.

Directe link
https://beveiligingsupdate.nl/2016/10/02/maarten-van-wieren-over-economische-spionage.

3.8. Tijdig ontdekken van datalekken

30-1-2017
Doelgroep
Medewerkers verantwoordelijk voor bescherming van de bedrijfsdata.
Beschrijving
Vaak hebben organisaties last van een datalek zonder dit te realiseren. Hoe dat komt en vooral wat je eraan kunt doen vertelt Ronald Kingma van Access42 aan Elleke Oosterwijk van het CIP.

Leerpunten
- Richt monitoring in;
- Analiseer je logging;
- Bepaal wat je kroonjuwelen zijn;
- Breng de keten in beeld;
- Welke tooling kun je privé gebruiken;
- Wat moet een bedrijf regelen.

Directe link
https://beveiligingsupdate.nl/2017/01/30/ronald-kingma-over-het-tijdig-ontdekken-van-datalekken/

3.9. Business Continuity management

9-2-2017
Doelgroep
Medewerkers verantwoordelijk voor bescherming van de bedrijfsdata.

Beschrijving
Business Continuity Management wat is het en wat kun je doen om na een incident meer zekerheid te hebben dat je vitale bedrijfsprocessen doorgang kunnen vinden. Rabih Lail vertelt aan Elleke Oosterwijk van CIP wat SVB heeft gedaan om BCM in te zetten en tegen welke uitdagingen je dan aanloopt.

Leerpunten
- Bepaal wat je vitale processen zijn;
- Maak scenario's voor het uitvallen van een onderdeel binnen deze processen;
- Oefen regelmatig.

Directe link
https://beveiligingsupdate.nl/2017/02/09/rabih-lail-over-business-continuity-management-oefenen-in-operationeel-blijven/

4. Bescherming hardware

4.1. Draadloze netwerken

1-10-2015
Doelgroep
Iedereen die gebruik van verschillende netwerken bv via een smartphone.

Beschrijving
Overal zijn er draadloze netwerken en iedereen maakt daar met verve gebruik van. Maar hoe veilig is dat en hoe kun je jezelf tegen risico's wapenen? Ronald Kingma van SecureLabs praat over de risico's en tips met Elleke Oosterwijk van het CIP. Wie veiliger wil zijn bij draadloze netwerk kan ook kijken op de pagina over draadloos van veiliginternetten.nl. Daarbij gaat het niet alleen over gebruik van draadloze netwerken, maar ook zijn er tips om zelf Wifi op te zetten.

Leerpunten
- Gebruik open netwerken alleen voor het benaderen van onbelangrijke websites;
- Hoe kan een crimineel pineapple inzetten om jouw sessie te kapen;
- Gebruik netwerken met een sterke encryptie;
- Zet het vinkje automatisch verbinding maken uit om niet steeds op onbeveiligde netwerken te komen waar je eerder toegang tot heb gehad;
- Gebruik bij voorbaat een VPN verbinding.

Directe link
https://beveiligingsupdate.nl/2015/10/01/ronald-kingma-over-draadloze-netwerken/

4.2. Het internet der dingen

20-11-2015
Doelgroep
Iedereen die gebruik maakt van slimme meters e.d.

Beschrijving
Wat betekent het dat we koelkasten, stereosets, slimme meters, thermostaten online beschikbaar maken en dus het internet der dingen bouwen? Zelf zien dat je veilig bent, is lastig te zien. Je moet er daarom op kunnen vertrouwen dat de leverancier heeft nagedacht over beveiliging en 'Security by Design' toepast. Aljo Houtman van Valori legt dat uit aan Brenno de Winter.

Leerpunten
- Update de apparaten die via internet verbonden zijn regelmatig;
- Probeer te achterhalen of de leverancier "security by design" heeft toegepast, vraag dit bij de aankoop van een apparaat;
- Wees voorzichtig omdat je nooit weet of de updates van de leveranciers ook de laatste bedreigingen tegenhoudt.

Directe link
https://beveiligingsupdate.nl/2015/11/20/aljo-houtman-het-internet-der-dingen/

4.3. Veilig mobiel werken

4-2-2016
Doelgroep
Iedereen die gebruik maakt van mobiele apparaten.

Beschrijving
Een belangrijk aspect bij het voorkomen van lekken is ons eigen gedrag. We hebben een flinke invloed door goed na te denken welke informatie we waar delen. Ook is het mogelijk om met simpele stappen onze apparatuur beter te beveiligen. Hoe dat kan legt Arjen Kamphuis, Lead Advisor information security, van Brunel uit aan Jan Renshof van het CIP.

Leerpunten
- Realiseer je wie meeluistert / -leest in openbare ruimtes;
- Versleutel de hard disk van je laptop, telefoon enz;
- Gebruik technieken om veilig gebruik te maken van open netwerken.

Directe link
https://beveiligingsupdate.nl/2016/02/04/arjen-kamphuis-over-veiliger-mobiel-werken/

4.4. Internationaal flexwerken

26-5-2016
Doelgroep
Iedereen die gebruik maakt van mobiele apparaten.

Beschrijving
Veel mensen nemen op vakantie hun mobiele telefoon, laptop enz. mee, om privé en zakelijk te gebruiken. Robert den Hartog legt vanuit Dubai via skype aan Elleke Oosterwijk van CIP uit welke maatregelen je kunt/moet nemen om te zorgen dat je apparaten en data niet in verkeerde handen vallen.

Leerpunten
- Leg je hardware aan een kabel of in de kluis op je hotelkamer;
- Encrypt je vaste schijf;
- Zorg dat je virusscanner etc up to date zijn;
- Zorg dat mensen niet met je mee kunnenluisteren;
- Zorg voor een screen protectors zodat mensen niet van opzij mee kunnen kijken;
- Encrypt je USB sticks.

Directe link
https://beveiligingsupdate.nl/2016/05/26/robert-den-hartog-internationaal-flexwerken/

4.5. De reinheid van je ICT apparatuur

9-6-2016
Doelgroep
Iedereen die gebruik maakt van mobiele apparaten.

Beschrijving
Of we nu thuis, op kantoor of onderweg werken, gegevens kunnen altijd in verkeerde handen vallen. Daarom moeten we altijd stil staan bij de hygiëne of reinheid van de computersystemen om misbruik te voorkomen. Wat een organisatie kan doen en waar we zelf verschil kunnen maken vertelt Harry Dragstra van DUO.

Leerpunten
- Laat je gezinsleden niet meekijken als je thuiswerk;
- Zorg dat er geen sporen op je privé laptop achterblijven als je een privé PC gebruikt;
- Zorg dat je de laatste update van de virusscanner installeert;
- Wees alert op phishing-mailtjes.

Directe link
https://beveiligingsupdate.nl/2016/06/09/harry-dragstra-de-reinheid-van-je-ict-apparatuur/

4.6. Omgaan met mobiele devices

13-10-2016
Doelgroep
Iedereen die gebruik maakt van mobiele apparaten.

Beschrijving
Door bedrijven en medewerkers wordt steeds meer gebruik gemaakt van mobiele apparaten. Zowel zakelijk als privé. Hoe kun je hier veilig mee omgaan. Meine van Essen van

Rijkswaterstaat geeft enkele tips. Eerder sprak Arjen Kamphuis over het vraagstuk waar werk je nou met welke informatie?

Leerpunten
- Een goede bescherming is om privé en zakelijk te scheiden;
- Controleer vóór installatie van een app welke rechten je deze app geeft;
- Meld altijd onmiddellijk wanneer een zakelijke mobiele device gestolen is.

Directe link
https://beveiligingsupdate.nl/2016/10/13/meine-van-essen-over-omgaan-met-mobiele-devices/

4.7. Find my phone

17-11-2016
Doelgroep
Alle bezitters van ee Android-telefoon.

Beschrijving
Per week wordt er in Nederland 300 keer aangifte gedaan van smartphone diefstal. Naast het feit dat je een dure telefoon kwijt bent, heeft een onbekende ook toegang tot al je foto's, video's, e-mails, contacten en berichten. Maar wat voor persoon steelt een telefoon? En waar komen die telefoons terecht? In de documentaire Find my Phone wordt het tweede leven van een gestolen telefoon gevolgd. Door middel van spyware maak je kennis met de persoon achter de diefstal. Maar hoe goed kun je iemand eigenlijk leren kennen aan de hand van zijn telefoon?

Leerpunten
- Welke mensen stelen telefoons;
- Waar komen gestolen telefoons zoal terecht;
- Wat kun je doen om na diefstal je telefoon te traceren.

Directe link
https://beveiligingsupdate.nl/2016/11/17/premiere-find-my-phone-anthony-van-der-meer/

5. Veilige software

5.1. Ontwikkelen van veilige apps

28-8-2015
Doelgroep
App ontwikkelaars.

Beschrijving
Met tablets en mobiele telefoons zijn apps populair. Ook bedrijven laten ze vaak maken om bedrijfsprocessen te ondersteunen. Want altijd en overal is bedrijfsinformatie beschikbaar. Als dat gebeurt komen er opeens allerlei beveiligings- en privacyrisico's bij kijken. Het is daarom belangrijk bij de totstandkoming van een app rekening te houden met de beveiliging en daar tijdig over na te denken. Marinus Kuivenhoven van Sogeti praat over het grip krijgen over apps met Brenno de Winter.

Leerpunten
- Bij het ontwikkelen moet je voor alle platforms vaststellen wat de zwakheden/bedreigingen zijn;
- Je moet weten waar de informatie uit de app wordt opgeslagen;
- Gebruik "grip op SSD" waarin de security eisen benoemd zijn;

- Prioriteer je beveiliging op basis van de risico's die de betreffende organisatie loopt.

Directe link
https://beveiligingsupdate.nl/2015/08/28/marinus-kuivenhoven-veilige-apps-maak-je-voor-je-gaat-bouwen/

6. Privacy

6.1. Denk na over privacy voordat je een systeem bouwt

17-9-2015
Doelgroep
Ontwikkelaars van informatiesystemen, processen, applicaties.

Beschrijving
Op 1 januari 2016 verandert de Wet bescherming persoonsgegevens. Privacy hoort dan op de radar van iedere organisatie te staan. Maar oplossing maak je niet op het laatste moment als het echt niet anders kan. Over privacy moet je vroegtijdig gaan nadenken vóór je systemen bouwt. Daarmee voorkomen we veel extra werk en kosten. Dat heet met een mooi woord Privacy by Design. Ric Gielen van Valori praat daarover met Robert den Hartog van het UWV.

Leerpunten
- Bedrijven willen zoveel mogelijk gegevens verzamelen omdat dat commercieel voordelig kan zijn;
- Privacy bij de start meenemen van de applicatieontwikkeling is veel goedkoper dan later je applicatie laten voldoen aan de privacy eisen;
- Neem de hele levenscyclus van een applicatie in ogenschouw, dus ook wanneer verwijder je de gegevens;
- Denk goed na over datafilters, dit kan je flexibeler maken.

- **Directe link**

https://beveiligingsupdate.nl/2015/09/17/ric-gielen-denk-over-privacy-voor-je-een-systeem-bouwt/

6.2. Privacy wetgeving omzetten in daden

3-3-2016
Doelgroep
Applicatieontwikkelaars.

Beschrijving
Om aan de eisen van de wet rond privacy te voldoen is voor veel organisaties behoorlijk lastig. Hoe weet je zeker of je echt aan de regels voldoet? En hoe kun je het voor elkaar krijgen om als organisatie echt privacy vriendelijk te zijn? Het CIP heeft een methode ontwikkeld om dat goed te regelen. Angelique van Oortmarssen legt aan Brenno de Winter uit hoe Grip op Privacy de wet omzet in concrete handelingen. Ook helpt de methodiek organisaties die privacy op een hoger niveau willen krijgen dan de wetgever verplicht. Met het gebruik van deze hulpmiddelen kunnen organisaties privacy binnen hun organisatie op een hoger niveau te brengen.

Leerpunten
- Grip op privacy helpt je aan de wet te voldoen;
- Als een organisatie privacy erg belangrijk vind kunnen ze het volwassenheidsniveau gebruiken, je moet minimaal aan niveau 3 voldoen om je aan de wet te houden, het halen van niveau 4 of 5 is dan een mogelijkheid;
- de privacy baseline heeft de WBP vertaalt naar concrete normen waarmee een applicatieontwikkelaar aan de slag kan;

- Privacy by design helpt je om vanaf de start van een ontwerp van een applicatie de privacy eisen mee te nemen;
- Je informatiehuishouding is op orde als je de privacy producten van CIP goed toepast. Dit voorkomt niet dat je een datalek kunt hebben maar dan is te onderbouwen dat je al het mogelijke hebt gedaan om dit te voorkomen.

Directe link
https://beveiligingsupdate.nl/2016/03/03/angelique-oortmarssen-privacywetgeving-omzetten-in-daden/

6.3. Privacyregels in de cloud

14-4-2016
Doelgroep
CISO, verantwoordelijken voor Informatiebeveiliging binnen de organisatie.

Beschrijving
Als je als organisatie gegevens wilt opslaan in de cloud waarop moet je dan letten en wat als je je gegevens weer uit de cloud wilt halen. Wat kun je doen als voorbereiding voor het geval er op termijn een datalek binnen je organisatie ontdekt wordt. Ot van Daalen geeft hierover een aantal tips aan Jan Renshof van het CIP.

Leerpunten
- Voor privacy gegevens moet je een compliance check waarin je analyseert welke gegevens je hebt wat je ermee doet en of je je aan de wet houdt;
- Als je gegevens in de cloud vastlegt moet je vaststellen onder welke wetgeving dat valt;
- Als je gegevens in de cloud opslaat moet je ook weten hoe je ze weer uit kunt halen;
- Je moet op voorhand een crisisteam inrichten die meteen kan handelen als er een datalek plaatsvindt, deze moeten een vooraf vastgesteld plan doorlopen;
- Na ieder datalek vaststellen of er aanpassingen binnen je organisatie moeten worden doorgevoerd.

Directe link
https://beveiligingsupdate.nl/2016/04/18/ot-van-daalen-privacyregels-in-de-cloud/

6.4. Tool self assessment privacy

11-5-2017
Doelgroep
Managers en medewerkers van afdelingen die persoonsgegevens verwerken, IB-functionarissen, Privacyofficer, FG'n.

Beschrijving
Het Centrum voor Informatiebeveiliging en Privacy bescherming heeft een tool ontwikkeld waarmee je, aan de hand van het gewenste volwassenheidsniveau van de organisatie, een self assesment kunt uitvoeren. Het resultaat geeft aan waar de organisatie staat en welke onderwerpen nog actie behoeven om aan het gewenste volwassenheidsniveau te voldoen. Marcel Koers en Ad Reuijl van CIP bespreken dit nieuwe product en geven aan welke behoefte het kan vervullen.

Leerpunten
- Welke producten heeft CIP in zijn portfolio om te helpen privacy bescherming op een hoger niveau te brengen;
- Hoe kun je als organisatie je volwassenheidsniveau vaststellen en wat is nodig om dit te bereiken;
- Hoe kun je de self assesment inzetten om Privacy als thema op de agenda te krijgen en bereik je awareness.

Directe link
https://beveiligingsupdate.nl/2017/05/11/marcel-koers-over-volwassenheid-op-privacy-gebied/

7. Identiteitsfraude

7.1. Identiteitsdiefstal

4-6-2015
Doelgroep
Iedere burger.

Beschrijving
Identiteitsdiefstal is een groeiend probleem. Vaak wordt daarbij ook misbruik gemaakt van identiteitsbewijzen. Dat is het moment waarop de Marechaussee vaak betrokken wordt. Kolonel Rob Koster van de Marechaussee is gespecialiseerd op fraude en praat erover met Jan Renshof van het Centrum voor Informatiebeveiliging en Privacybescherming. Wat moet je doen om de kans op misbruik te verminderen?

Leerpunten
- Deel geen identiteitsbewijzen op social media;
- Wat je niet weggeeft kun je niet kwijtraken;
- Bescherm je data;
- Controleer dat degene met wie je zaken doet echt is wie hij zegt dat hij is;
- Doe aangifte als je denkt dat persoonsgegevens van je gestolen zijn.

Directe link
https://beveiligingsupdate.nl/2015/06/04/rob-koster-van-de-marechaussee-over-identiteitsdiefstal/

8. De Cloud

8.1. Veiliger werken in de Cloud

28-4-2016
Doelgroep
Iedereen die data in de Cloud zet.

Beschrijving
Organisaties slaan meer en meer gegevens op in de cloud, verwerken administraties en versturen gegevens via de cloud. Is dat wel veilig? Welke keuzes maakt DUO daarin om de informatieveiligheid te vergroten? Beveiligingsexpert Harry Dragstra legt dat uit aan Brenno de Winter.

Leerpunten
- Organisaties kunnen met Cloud leveranciers contractueel vastleggen dat ze pentesten uitvoeren op de dienstverlening;
- Je kunt gegevens beter geencrypt in de cloud opslaan;
- Als je gebruik maakt van een Cloud leverancier moet je goed naar de voorwaarden kijken. Als de Cloud leverancier failliet gaat wil je je gegevens wel terug krijgen;
- Controleer of je Cloud leverancier gecertificeerd is, in dat geval heeft hij in ieder geval een aantal beveiligingsmaatregelen geïmplementeerd.

Directe link

https://beveiligingsupdate.nl/2016/05/12/harry-dragstra-veiliger-werken-in-de-cloud/

9. Social media

9.1. Social media

7-7-2016
Doelgroep
Iedereen die gebruik maakt van social media.

Sociale media zijn voor veel mensen zowel privé als zakelijke een vast onderdeel van het dagelijks leven. We wisselen informatie uit, hebben een mening en soms werk dat het net ingewikkeld maakt om daar goed mee om te gaan. Waar moet je allemaal rekening mee houden? En ooit komt de onvermijdelijke dag dat je het niet goed doet. Hoe ga je daarmee om? Dat vertelt Marieke van der Klaauw, van het Openbaar Ministerie.

Leerpunten
- Denk na voordat je wat deelt op social media;
- Besef welke uitstraling je hebt op social media
- Kijk goed naar je privacy instellingen
- Weet wat er over jezelf op social media te vinden is.

Directe link
https://beveiligingsupdate.nl/2016/07/11/marieke-van-der-klaauw-verstandig-omgaan-met-sociale-media/

10. Diverse

10.1. CIP

31-3-2016
Doelgroep
Iedereen die geïnteresseerd is in CIP.

Beschrijving
De Beveiligingsupdate is een CIP-Cast om daarmee een knipoog te maken naar het Centrum voor Informatiebeveiliging en Privacybescherming. Regelmatig komt de vraag langs wat deze organisatie nou is en doet. Daarom een aflevering om dat uit te leggen.
Het CIP werd in 2012 opgericht als een breed netwerk met zowel publieke als private partijen. In deze aflevering legt Ad Reuijl aan Elleke Oosterwijk uit wat het CIP allemaal beschikbaar heeft. Tevens vertelt Ad hoe CIP werkt en hoe organisaties kunnen aansluiten. Het credo is "van allen voor allen".

Leerpunten
- CIP komt voort uit het programma Compacte Rijksoverheid;
- Iedereen kan meedoen bij CIP, zowel overheidspartijen als commerciële bedrijven;
- CIP stelt zijn producten "om niet" beschikbaar;
- Ook vragen op het gebied van Informatiebeveiliging kun je door het CIP netwerk laten beantwoorden;
- Doel is Nederland veiliger maken.

Directe link
https://beveiligingsupdate.nl/2016/03/30/ad-reuijl-beveiliging-voor-allen-door-allen/

10.2. Een vrij beschikbare bewustwordingstraining

1-9-2016
Doelgroep
Iedereen die geen security specialist is.

Beschrijving
Ieder bedrijf hoort aan bewustwording binnen de organisatie te doen. Dat is niet alleen een onderdeel van beveiligingsnormen, maar ook noodzakelijk om ieder beleid kansrijk te maken. Personeel zal dus moeten worden getraind. Radically Open Security ontwikkelt producten die vrij beschikbaar zijn om te gebruiken en ontwikkelden een bewustwordingstraining in opdracht van een van hun klanten.
De training is kosteloos en herbruikbaar beschikbaar. Hoe dat werkt vertelt Melanie Rieback, de oprichter van het bedrijf, aan Ad Reuijl van het CIP.

Leerpunten
Een bewustwordingscampagne opzetten hoeft niet veel geld te kosten er is geen gratis oplossing.

Directe link
https://beveiligingsupdate.nl/2016/09/01/een-vrij-beschikbare-bewustwordingstraining/

10.3. Mensen overtuigen om gedrag aan te passen

1-12-2016
Doelgroep
Communicatiemedewerkers verantwoordelijk voor het verhogen van awareness binnen de organisatie

Beschrijving
Informatiebeveiliging, zowel zakelijk als privé, is erg belangrijk in dit digitale tijdperk. Mensen zien activiteiten op dit vlak vaak als opgelegd in plaats van dat ze zelf het nut ervan inzien en dus veilig gedrag willen vertonen. Patricia van Schaik en Jaco Koetsveld wat je kunt doen om mensen intrinsiek veiliger gedrag te laten vertonen.

Leerpunten
- Moeten ombuigen naar willen;
- Handreikingen geven aan mensen uit het primair papieren tijdperk;
- Regelmatig metingen doen en resultaat terugleggen.

Directe link
https://beveiligingsupdate.nl/2016/12/01/mensen-overtuigen-om-gedrag-aan-te-passen/

10.4. Terugblik 2016

15-12-2016
Doelgroep
Iedereen die geïnteresseerd is in de producten van CIP.

Beschrijving

Ad Reuijl en Brenno de Winter kijken terug op 2016, welke ontwikkeling heeft CIP doorgemaakt en welke producten zijn beschikbaar gesteld om de BV Nederland "informatie veiliger" te maken. Tevens kijken zij vooruit en vertellen iets over de plannen voor 2017.

Leerpunten
- Wat zijn de belangrijkste wapenfeiten van CIP in 2016:
- Welke producten gaat CIP in 2017 verder ontwikkelen.

Directe link
https://beveiligingsupdate.nl/2016/12/21/terugblik-2016-vooruitblik-2017/

10.5. Hoe krijg je beveiliging op een hoger niveau

23-2-2017
Doelgroep
Bestuurders en betrokkenen bij informatiebeveiliging.

Beschrijving
Jaap Halfweeg, CISO bij de Sociale Verzekeringsbank (SVB), gooit het roer om. Veel organisaties hebben een focus op vooral het voorkomen van incidenten. Dat is voor hem niet genoeg. Iedere organisatie krijgt met regelmaat met incidenten te maken. De vraag is hoe informatiebeveiliging op een hoger niveau komt en hoe dat in het beveiligingsbeleid dan weerslag krijgt. Jaap deelt zijn ervaring over die worsteling met Brenno de Winter.

Leerpunten
- Cyberdreiging en complexiteit nemen toe;
- Van incidenten voorkomen naar monitoren en daarop reageren;
- Leer van incidenten en bijna incidenten.

Directe link
https://beveiligingsupdate.nl/2017/02/28/jaap-halfweeg-hoe-krijg-je-beveiliging-op-een-hoger-niveau/