



Zie voor laatste CIP-cast: <https://beveiligingsupdate.nl/>

CIP-CAST PORTFOLIO

**Klik in de inhoudsopgave om
direct naar de CIP-Cast van uw keuze te gaan.**

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan echter voorkomen dat er toch sprake is van omissies of onjuistheden. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie.



© Centrum voor Informatiebeveiliging en Privacybescherming.
Voor dit werk geldt een Creative Commons Naamsvermelding GelijkDelen 4.0
verleend door het CIP. Zie <http://creativecommons.org/licenses/by-sa/4.0/>

Inhoud

1.	Inleiding	4
1.1.	Centrum voor Informatiebeveiliging en Privacybescherming (CIP)	4
1.2.	CIP -Casts	4
2.	E-Mail	5
2.1.	Nepmails van de bank en Phishing via e-mail	5
2.2.	Test met Phishing mail binnen een organisatie	5
2.3.	Veiliger versturen van e-mail	6
2.4.	Omgaan met phishing	6
2.5.	Veilig e-mailgebruik	7
3.	Datalekken	8
3.1.	Meldpunt datalekken	8
3.2.	Ik heb een datalek. Wat nu?	8
3.3.	Hoe om te gaan met een Cryptolocker	9
3.4.	Vorbereiden op een datalek	9
3.5.	Wie helpt nu met wat bij informatiebeveiliging?	10
3.6.	Communiceren over een datalek	10
4.	Gegevens	12
4.1.	Encryptie of versleuteling	12
4.2.	Als je data op straat ligt	12
4.3.	Voorwaarden om persoonsgegevens te verwerken	13
4.4.	Bewaren van gegevens	13
4.5.	Classificeren van gegevens	14
4.6.	Economische spionage	14
4.7.	Tijdig ontdekken van datalekken	15
4.8.	Business Continuity management	15
5.	Bescherming hardware	16
5.1.	Draadloze netwerken	16
5.2.	Veilig mobiel werken	16
5.3.	Internationaal flexwerken	17
5.4.	De reinheid van je ICT apparatuur	17
5.5.	Omgaan met mobiele devices	18
5.6.	Find my phone	18
6.	Veilige software	19
6.1.	Ontwikkelen van veilige apps	19
7.	Privacy	20
7.1.	Denk na over privacy voordat je een systeem bouwt	20
7.2.	Privacy wetgeving omzetten in daden	20
7.3.	Privacyregels in de Cloud	21

7.4. Tool self assessment privacy	21
8. Identiteitsfraude	23
8.1. Identiteitsdiefstal	23
9. De Cloud.....	24
9.1. Veiliger werken in de Cloud	24
10. Social media	25
10.1. Social media.....	25
11. Diversen.....	26
11.1. Beveiliging voor allen door allen.....	26
11.2. Een vrij beschikbare bewustwordingstraining	26
11.3. Mensen overtuigen om gedrag aan te passen	27
11.4. Terugblik 2016	27
11.5. Hoe krijg je beveiliging op een hoger niveau.....	28
11.6. Informatiebeveiliging op orde hebben en houden	28
11.7. Economische spionage.....	29
11.8. Mó fáng	29
11.9. Fysieke beveiliging van informatie.....	30

1. Inleiding

1.1. Centrum voor Informatiebeveiliging en Privacybescherming (CIP)

CIP is het expertiseCentrum voor Informatiebeveiliging en Privacybescherming van, voor en door overheidsorganisaties. Het heeft zich ontwikkeld tot een publiek/private netwerkorganisatie, waarin ook deskundige marktorganisaties als kennispartners deelnemen.

Het CIP is opgericht door vier grote uitvoeringsorganisaties: Belastingdienst, DUO, SVB en UWV. Inmiddels bestaat het CIP-netwerk uit een groot aantal overheidsorganisaties en Kennispartners. Kennis die in deze organisaties aanwezig is op het vlak van informatiebeveiliging en privacybescherming wordt binnen de samenwerking in het CIP gedeeld en toegankelijk gemaakt. Op deze manier leren de aangesloten organisaties van elkaars oplossingen en werkwijzen en kunnen, samen komen tot afspraken daaromtrent dit onderwerp. Dit alles in het belang van het verhogen van de informatieveiligheid van de overheidsdienstverlening.

Door binnen de overheid meer samen te gaan doen, draagt het CIP ook bij aan het optimaal gebruik van overheidsmiddelen.

1.2. CIP -Casts

CIP stelt korte filmpjes beschikbaar die door iedere organisatie ingezet kunnen worden om de informatieveiligheid te verhogen. De filmpjes duren in het algemeen maximaal 5 minuten. Deze filmpjes noemen we CIP-Casts. Deze CIP-Casts kunnen ook door individuele burgers bekeken worden om hen te helpen in de privéomgeving de informatieveiligheid te verhogen.

De filmpjes bevatten veelal interviews waarin maatregelen tegen dreigingen worden besproken.

In deze portfolio staat op onderwerp een toelichting op de CIP-Casts. Met deze onderverdeling kan makkelijk gezocht worden of er een geschikte CIP-Cast tussen zit. Bovendien kan er makkelijk doorgelinkt 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, de speelduur en welke leerpunten eruit gehaald kunnen worden. Indien van toepassing en bekend zijn ook links in de tekst toegevoegd om snel meer informatie te krijgen. Aan de datum kun je zien wanneer deze CIP-Cast gepost is op <https://www.beveiligingsupdate.nl/>.

2. E-Mail

2.1. Nepmails van de bank en Phishing via e-mail

2-7-2015

Doelgroep

Iedereen die e-mail gebruikt.

Speelduur

4 minuten en 13 seconden.

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 internetbankieren](#) 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/>

2.2. Test met Phishing mail binnen een organisatie

16-7-2015

Doelgroep

Iedereen die een phishing campagne wil opzetten.

Speelduur

3 minuten en 34 seconden.

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 trapt 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 een phishing-actie opzet.

Directe link

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

2.3. Veiliger versturen van e-mail

14-8-2015

Doelgroep

Iedereen die meer wil weten over het belang van e-mail encryptie.

Speelduur

2 minuten en 50 seconden.

Beschrijving

Als je een e-mailbericht stuurt. Hoe veilig is dat eigenlijk? Vaak voelt dat vertrouwt aan. Maar kunnen andere partijen meelesen 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/>

2.4. Omgaan met phishing

30-10-2016

Doelgroep

Organisaties die zich willen wapenen tegen phishing e-mails.

Speelduur

5 minuten en 19 seconden.

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.

Directe link

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

2.5. Veilig e-mailgebruik

6-4-2016**Doelgroep**

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

Speelduur

4 minuten en 50 seconden.

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 Cloud-server;
- Een e-mail is qua openbaarheid vergelijkbaar met een briefkaart;
- Maak gebruik van versleuteling.

Directe link

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

3. Datalekken

3.1. Meldpunt datalekken

30-7-2015

Doelgroep

Iedereen die verantwoordelijk is voor de gegevenshuishouding.

Speelduur

3 minuten en 53 seconden.

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/>

3.2. Ik heb een datalek. Wat nu?

18-2-2016

Doelgroep

Iedereen die verantwoordelijk is voor de gegevenshuishouding.

Speelduur

5 minuten en 7 seconden.

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/>

3.3. Hoe om te gaan met een Cryptolocker

17-3-2016

Doelgroep

Iedereen die data beheert.

Speelduur

5 minuten en 43 seconden.

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/>

3.4. Voorbereiden op een datalek

18-3-2017

Doelgroep

Leden van crisisteams die ingezet worden wanneer een datalek een feit is.

Speelduur

5 minuten en 23 seconden.

Beschrijving

Iedere organisatie wordt wel 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/>

3.5. Wie helpt nu met wat bij informatiebeveiliging?

20-4-2017

Doelgroep

Iedereen die zich bezig houdt met informatiebeveiliging, crisisteam informatiebeveiliging.

Speelduur

5 minuten en 58 seconden.

Beschrijving

Het Nationale Cyber Security Centrum (NCSC) en de Informatiebeveiligingsdienst (IBD) helpen organisaties wanneer een incident rond informatiebeveiliging optreedt. Maar wie doet nu wat en wat mag je van welke organisatie verwachten? NCSC richt zich daarbij primair op het Rijk en de vitale sectoren en IBD op de gemeenten. NCSC en IBD kunnen organisaties helpen bij het melden van incidenten maar ook in de juiste richting wijzen bij het afhandelen van een incident. 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/>

3.6. Communiceren over een datalek

6-6-2017

Doelgroep

Bestuurders en communicatiedeskundigen (primair gemeenten).

Speelduur

5 minuten en 12 seconden.

Beschrijving

Als de buitenwereld, via de media, aangeeft dat jouw organisatie verantwoordelijk is voor een datalek, moet je de oorzaak dan eerst uitzoeken of meteen communiceren en welke strategie kun je dan het best hanteren. Remco Groet van de Informatiebeveiligingsdienst (IBD) gaat in gesprek met Brenno de Winter en vertelt welke adviezen zij hierover geven aan de gemeenten.

Leerpunten

- Wanneer moet je communiceren;
 - Als de dienstverlening in het geding is;
 - Als persoonsgegevens in het geding zijn;
- Als er grote financiële gevolgen (te verwachten) zijn;
 - Neem zelf het initiatief/voortouw;

- Maak de informatie voor iedereen toegankelijk.

Directe link

<https://beveiligingsupdate.nl/2017/06/06/remco-groet-communiceren-over-een-datalek/>

4. Gegevens

4.1. Encryptie of versleuteling

18-6-2015

Doelgroep

Iedereen die haar/zijn informatiebeveiliging wil verhogen.

Speelduur

5 minuten en 5 seconden.

Beschrijving

Bij het beveiligen van onze informatie verwerkingsomgeving wordt gesproken over encryptie en versleuteling. Wat is dat nou? Hoe werkt het? Waarom hebben is dat nodig om informatie te versleutelen? Wat betekenen termen als symmetrische versleuteling, asymmetrische versleuteling, PGP en S/MIME? Hans de Raad van OpenNovations legt dit uit aan Ad Reuijl van het CIP.

Leerpunten

- Wat is encryptie/versleuteling;
- Hoe werkt het;
- Wat is het verschil tussen symmetrische en asymmetrische 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/>

4.2. Als je data op straat ligt

16-10-2015

Doelgroep

Informatiebeveiliging specialisten. Iedereen die veilig van websites gebruik wil maken.

Speelduur

3 minuten en 52 seconden.

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 zetten 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/>

4.3. Voorwaarden om persoonsgegevens te verwerken

3-12-2016

Doelgroep

Iedereen die persoonsgegevens bewerkt.

Speelduur

4 minuten en 53 seconden.

Beschrijving

Een organisatie die persoonsgegevens wil verwerken moet zich aan een aantal regels houden. Zij moeten vooraf over zaken nadenken. Maar dat is zo algemeen en niet helder. Vanaf 1 januari 2016 kunnen boetes worden uitgedeeld wanneer de wet (WBP) overtreden wordt. Wat zijn de belangrijkste dingen waar je op moet 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/>

4.4. Bewaren van gegevens

18-12-2016

Doelgroep

Iedereen die data beheert.

Speelduur

4 minuten en 50 seconden.

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 afgeschermd 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/>

4.5. Classificeren van gegevens

19-9-2016

Doelgroep

Iedereen die data beheert.

Speelduur

3 minuten en 34 seconden.

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/>

4.6. Economische spionage

29-9-2016

Doelgroep

Iedereen verantwoordelijk voor bescherming van de bedrijfsdata.

Speelduur

3 minuten en 19 seconden.

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 hierin 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.>

4.7. Tijdig ontdekken van datalekken

30-1-2017

Doelgroep

Medewerkers verantwoordelijk voor bescherming van de bedrijfsdata.

Speelduur

5 minuten en 34 seconden.

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;
- Analyseer 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/>

4.8. Business Continuity management

9-2-2017

Doelgroep

Iedereen verantwoordelijk voor bescherming van de bedrijfsdata.

Speelduur

3 minuten en 48 seconden.

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/>

5. Bescherming hardware

5.1. Draadloze netwerken

1-10-2015

Doelgroep

Iedereen die gebruik van verschillende netwerken bv via een smartphone.

Speelduur

4 minuten en 7 seconden.

Beschrijving

Overall zijn 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/>

5.2. Veilig mobiel werken

4-2-2016

Doelgroep

Iedereen die gebruik maakt van mobiele apparaten.

Speelduur

5 minuten en 7 seconden.

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/>

5.3. Internationaal flexwerken

26-5-2016

Doelgroep

Iedereen die gebruik maakt van mobiele apparaten.

Speelduur

3 minuten en 48 seconden.

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 kunnen luisteren;
- 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/>

5.4. De reinheid van je ICT apparatuur

9-6-2016

Doelgroep

Iedereen die gebruik maakt van mobiele apparaten.

Speelduur

4 minuten en 39 seconden.

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/>

5.5. Omgaan met mobiele devices

13-10-2016

Doelgroep

Iedereen die gebruik maakt van mobiele apparaten.

Speelduur

3 minuten en 47 seconden.

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 aan Elleke Oosterwijk van het CIP.

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/>

5.6. Find my phone

17-11-2016

Doelgroep

Iedereen die gebruik maakt van een Android-telefoon.

Speelduur

21 minuten en 29 seconden.

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/>

6. Veilige software

6.1. Ontwikkelen van veilige apps

28-8-2015

Doelgroep

Opdrachtgevers voor app ontwikkelaars.

Speelduur

4 minuten en 33 seconden.

Beschrijving

Met het gebruik van tablets en mobiele telefoons zijn apps populair geworden. Ook bedrijven laten vaak apps maken om bedrijfsprocessen te ondersteunen. Want dan is altijd en overal het bedrijfsinformatie en dus de bijbehorende informatie beschikbaar. Er moet echter wel rekening gehouden worden met allerlei beveiligings- en privacy risico's die hierdoor ontstaan. 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;
- SSD helpt de dialoog tussen opdrachtgever en de app ontwikkelaar op gang te brengen en legt de focus op de juiste security eisen;
- 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/>

7. Privacy

7.1. Denk na over privacy voordat je een systeem bouwt

17-9-2015

Doelgroep

Iedereen die informatiesystemen, processen, applicaties ontwikkelt.

Speelduur

4 minuten en 58 seconden.

Beschrijving

Op 1 januari 2016 verandert de Wet bescherming persoonsgegevens. Privacy hoort dan op de radar van iedere organisatie te staan. Oplossingen ontwikkelen die voldoen aan de wet gaat niet vanzelf. Over Privacy moet je nadenken bij de start van de ontwikkeling van een informatiesysteem. Dit voorkomt herstelacties en kosten achteraf. Dat heet met een mooi woord Privacy by Design. Ric Gielen van Valori praat daarover met Robert den Hartog van het UWV.

Leerpunten

- De wet stelt eisen aan welke gegevens verzamelt mogen worden;
- 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/>

7.2. Privacy wetgeving omzetten in daden

3-3-2016

Doelgroep

Opdrachtgevers van applicatieontwikkelaars/bestuurder.

Speelduur

5 minuten en 1 seconde.

Beschrijving

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? Wat moet je doen 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 je met [Grip op Privacy](#) de wet kunt omzetten in concrete handelingen. Met het gebruik van deze methodiek kunnen organisaties privacy binnen hun organisatie op een hoger niveau te brengen.

Leerpunten

- Als een organisatie ben je wettelijk verplicht iets aan privacy te doen;
- Grip op privacy helpt je aan de wet te voldoen;
- 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/>

7.3. Privacyregels in de Cloud

18-4-2016**Doelgroep**

Iedereen verantwoordelijk voor Informatiebeveiliging binnen de organisatie, CISO.

Speelduur

5 minuten en 3 seconden.

Beschrijving

Hoe kun je je voorbereiden op het risico van een datalek.

Wanneer 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 het waarborgen van de privacy van gegevens moet je een compliance check doen, 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/>

7.4. Tool self assessment privacy

11-5-2017**Doelgroep**

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

Speelduur

2 minuten en 41 seconden.

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/>

8. Identiteitsfraude

8.1. Identiteitsdiefstal

4-6-2015

Doelgroep

Iedere burger.

Speelduur

4 minuten en 10 seconden.

Beschrijving

Identiteitsdiefstal is een groeiend probleem. Vaak wordt daarbij ook misbruik gemaakt van identiteitsbewijzen. Dat is het moment waarop de Marechaussee veelal 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/>

9. De Cloud

9.1. Veiliger werken in de Cloud

12-5-2016

Doelgroep

Iedereen die data in de Cloud zet.

Speelduur

5 minuten en 41 seconden.

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.

Zie ook de CIP cast "Privacyregels in de Cloud" waarin Ot van Daalen de regels toelicht.

Leerpunten

- Organisaties kunnen met Cloud leveranciers contractueel vastleggen dat ze pentesten uitvoeren op de dienstverlening;
- Awareness van medewerkers is belangrijk "denk na welke dat je deelt".
- Je kunt gegevens beter ge-encrypt 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/>

10. Social media

10.1. Social media

7-7-2016

Doelgroep

Iedereen die gebruik maakt van social media.

Speelduur

3 minuten en 40 seconden.

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 geven zo dus veel informatie vrij. Hoe kun je hier goed mee omgaan.. 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 aan Brenno de Winter.

Leerpunten

- Denk na voordat je iets 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/>

11. Diversen

11.1. Beveiliging voor allen door allen

30-3-2016

Doelgroep

Iedereen die geïnteresseerd is in CIP.

Speelduur

4 minuten en 5 seconden.

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/>

11.2. Een vrij beschikbare bewustwordingstraining

1-9-2016

Doelgroep

Iedereen die geen security specialist is.

Speelduur:

3 minuten en 3 seconden.

Beschrijving

Ieder bedrijf hoort aan bewustwording tav informatiebeveiliging, 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.

Leerpunt

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/>

11.3. Mensen overtuigen om gedrag aan te passen

1-12-2016

Doelgroep

Iedereen verantwoordelijk voor het verhogen van awareness binnen de organisatie vanuit de communicatiekant.

Speelduur

3 minuten en 41 seconden.

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 vertellen aan Brenno de Winter 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/>

11.4. Terugblik 2016

15-12-2016

Doelgroep

Iedereen die geïnteresseerd is in de producten van CIP.

Speelduur

4 minuten en 35 seconden.

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-voorblik-2017/>

11.5. Hoe krijg je beveiliging op een hoger niveau

28-2-2017

Doelgroep

Iedereen die betrokken is bij en belang hecht aan informatiebeveiliging.

Speelduur

4 minuten en 9 seconden.

Beschrijving

Jaap Halfweg, 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-halfweg-hoe-krijg-je-beveiliging-op-een-hoger-niveau/>

11.6. Informatiebeveiliging op orde hebben en houden

4-10-2017

Doelgroep

Medewerkers verantwoordelijk voor de informatieveiligheid van organisaties

Speelduur

4 minuten en 51 seconden.

Beschrijving

Hoe krijg je je informatiebeveiliging op orde en hoe toon je dat aan. Kees en Jule Hintzbergen (IBD) zijn al jaren bezig in dit vakgebied bij de gemeenten en vertellen aan Brenno de Winter welke ervaringen zij in de loop der jaren hebben opgedaan en hoe informatiebeveiliging zich ontwikkelt.

Leerpunten

- Spreek in een keten een beveiligingsniveau af;
- Gebruik een baseline BIR, BIG enz.;
- Voer een Gap analyse uit om te bepalen op welke normen nog actie nodig is;
- Bepaal welke risico's voor jouw organisatie het belangrijkste zijn;
- Pas, indien nodig, de maatregelen aan na een incident of wetswijziging.

Directe link

<https://beveiligingsupdate.nl/2017/10/04/gebroeders-hintzbergen-informatiebeveiliging-op-orde-hebben-en-houden/>

11.7. Economische spionage

31-10-2017

Doelgroep

Management en security officers van bedrijven waar veel innovatieve kennis beschikbaar is.

Speelduur

3 minuten en 33 seconden.

Beschrijving

Wat is economische spionage? Wat kan het voor je betekenen? Wat kun je ertegen doen? Erik de Jong van Fox-IT heeft veel ervaring opgedaan over dit onderwerp en deelt dit met Brenno de Winter.

Leerpunten

- Beveilig de producten in ontwikkeling voordat ze op de markt komen;
- De aanvaller heeft altijd veel tijd om de informatie te achterhalen;
- Versleutel je informatie;
- Gebruik 2 stappen verificatie;
- Denk na over uitbesteding van informatiebeveiliging als je de kennis niet in huis hebt.

Directe link

<https://beveiligingsupdate.nl/2017/10/31/erik-de-jong-over-economische-spionage/>

11.8. Mó fáng

23-11-2017

Doelgroep

Management en security officers van bedrijven waar veel innovatieve kennis beschikbaar is.

Speelduur

5 minuten en 6 seconden.

Beschrijving

Hoe werkt economische spionage? Mó fáng is een Chinese groepering die zich richt op economische spionage. Erik de Jong van Fox-it legt aan Brenno de Winter hoe Mó fáng te werk gaat.

Leerpunten

- Economische spionage is een langlopende operatie;
- APT Advanced Persistent Threat
- Breng je medewerkers op de hoogte van mogelijke economische spionage.

Directe link

<https://beveiligingsupdate.nl/2017/12/04/erik-de-jong-over-economische-spionage-het-mo-fang-onderzoek/>

11.9. Fysieke beveiliging van informatie

29-1-2018

Doelgroep

Medewerkers belast met fysieke en technische informatie beveiliging.

Speelduur

3 minuten en 11 seconden.

Beschrijving

Tom Smits van Fox-it vertelt aan Elleke Oosterwijk van het CIP welke fysieke maatregelen je in kunt zetten om de technische maatregelen voor informatie beveiliging te ondersteunen.

Leerpunten

- Zorg bij beveiliging voor een gelaagd model
- Geef mensen verschillende kleuren passen om snel te kunnen beoordelen of iemand ongeautoriseerd in een ruimte aanwezig is.
- Stel per medewerker vast welke data ze mogen benaderen
- Versleutel je data voordat het je netwerk verlaat
- Neem niet onnodig data het bedrijfspan uit.

Directe link

<https://beveiligingsupdate.nl/2018/01/29/tom-smits-over-fysieke-beveiliging-van-informatie/>