



Swinth IvO-Partners

Uw kennispartner voor informatieveiligheid en privacy beleid





Swinth IvO-Partners

Uw kennispartner voor informatieveiligheid en privacy beleid

**Hoe gaat GGZ-instelling Emergis
om met informatie beveiliging en de
Europese privacy verordening?**

Inhoud

1. Introductie
2. Informatieveiligheid en privacy van alle kanten bedreigd
3. Het belang van privacy en informatieveiligheid; er kan veel misgaan
4. Aanpak van informatiebeveiliging en privacybeleid binnen Emergis
5. Enkele tips en adviezen

1. Introductie





Ad Koppejan

Directeur/oprichter Swinth / IvO-Partners

Jarenlange ervaring met ICT gerelateerde opdrachten voor overheid en bedrijfsleven. Sinds 2013 actief met verbeteren informatieveiligheid en privacybeleid

Van 2006 tot medio 2012 lid van de Tweede Kamer

Voorzitter Raad van Toezicht van GGZ-instelling Emergis in Zeeland



- Breed zorgaanbod in de GGZ
- $\pm$ 11.000 cliënten
- $\pm$ 1.400 medewerkers
- 99,7 miljoen omzet in 2016
- Werkgebied: Zeeland





Ooops, your files have been encrypted!

Dutch

Wat is er gebeurd met deze computer?

Uw belangrijke bestanden zijn versleuteld.

Veel van uw documenten, foto's, video's, databases en andere bestanden zijn niet meer toegankelijk omdat ze gecodeerd zijn. Misschien ben je bezig met het zoeken naar een manier om je bestanden te herstellen, maar verspil je tijd niet. Niemand kan uw bestanden herstellen zonder onze decryptiedienst.

Kan ik mijn bestanden herstellen?

Zeker. Wij garanderen dat u al uw bestanden veilig en gemakkelijk kunt herstellen. Maar je hebt niet zo genoeg tijd.

U kunt gratis gratis decoderen van uw bestanden. Probeer nu <Decrypt> te klikken. Maar als u al uw bestanden wilt decoderen, moet u betalen.

U heeft slechts 3 dagen om de betaling in te dienen. Daarna wordt de prijs verdubbeld. Ook als u niet over 7 dagen betaalt, kunt u uw bestanden voor altijd niet herstellen.

We hebben gratis evenementen voor gebruikers die zo arm zijn dat ze niet in 6 maanden kunnen betalen.

Hoe betaal ik?

Betaling wordt alleen in Bitcoin geaccepteerd. Klik voor meer informatie op <About bitcoin>.

Controleer de huidige prijs van Bitcoin en koop een aantal bitcoins. Klik voor meer informatie op <How to buy bitcoins>.

En stuur het juiste bedrag naar het adres dat in dit venster is opgegeven.

Payment will be raised on

5/15/2017 17:36:51

Time Left

02:23:50:54

Your files will be lost on

5/19/2017 17:36:51

Time Left

06:23:50:54



Nieuws



Zeven Britse ziekenhuizen nog ontregeld door WannaCry

maandag 15 mei 2017, 13:51 door Redactie, 7 reacties

Zeven Britse
problemen te
geannuleerd



Zondag 02 juli 2017 Het laatste nieuws het eerst op NU.nl



Het gaat onder andere om **Barts** ambulances naar andere ziekenhuizen patiënten die voor vandaag stonden. **National Health Service (NHS)** oude Windowsversie te vervangen.

De NHS adviseerde zorgpersoneel konden worden aangezet. Verder kan worden voorkomen. In het geval van loskoppelen en via het terugplaatsen.

- Microsoft publiceert beveiligingsupdates
- Toegangscode cockpitdeuren Units

Voorpagina

Net binnen

Algemeen

Binnenland

Buitenland

Politiek

NUweekend

Economie

Zakelijk

Sport

Tech

Entertainment

Lifestyle

Overig

Video's

Regionaal

NU.nl > Algemeen



'Zeker vijftien Nederlandse ziekenhuizen geïnfecteerd met ransomware'

Gepubliceerd: 25 juni 2017 17:34

Laatste update: 25 juni 2017 18:14

Zeker vijftien Nederlandse ziekenhuizen zijn in de afgelopen tijd geïnfecteerd met ransomware. Dat blijkt uit een rondgang onder vijftientwintig ziekenhuizen door de NOS. In één van die ziekenhuizen werden 75 computers geïnfecteerd.



tweakers

Nieuws

Reviews

Pricewatch

Vraag & Aanbod

Forum

Meer

Inloggen

Gegevens 2385 patiënten AMC-ziekenhuis lagen op straat

Door Olaf van Miltenburg, 28 februari 2017 21:01 • 78 reacties • Feedback • f in t

Gegevens van 2385 patiënten van het Academisch Medisch Centrum in Amsterdam waren in te zien dankzij een kwetsbaarheid bij een pagina van een derde partij. Naast naw-gegevens ging het om onder andere burgerservicenummers, verzekeringsgegevens en afspraken.

Het lek betrof het online inschrijfformulier van de polikliniek Mondziekten, Kaak- en Aangezichtschirurgie van het AMC. De kwetsbaarheid kwam vorige week vrijdag aan het licht toen Nelson Berg van beveiligingsbedrijf BinaryIT online een afspraak bij het AMC moest maken om zijn verstandskies te laten trekken. "Ik ben nieuwsgierig en loop dan soms even de beveiliging na. Dankzij een waarschuwing op de site en met behulp van sqlmap kreeg ik via sql-injectie toegang tot een database met 3500 records", vertelt Berg aan Tweakers.

HOE AC
JE DE
ONDER
VAN DE
ARBEID
MARKT
DOWNI

Map.norsecorp.com



TECH

Zorg treuzelt met informatiebeveiliging

Philip van de Poel

26 januari 2017

2318 keer gelezen

0 reacties



Zorginstellingen maken nog onvoldoende vaart op het gebied van informatiebeveiliging. Hoewel er vooruitgang is geboekt zijn de meeste instellingen nog lang niet klaar voor de introductie van de Europese Privacy-verordening (EPV) in 2018.

Belangrijkste uitkomsten onderzoek BDO naar informatiebeveiliging in de zorg

Van alle Nederlandse zorginstellingen:

- is 50% bekend met Europese Privacy verordening
- heeft 49% nog geen beleid om privacy van cliënten te kunnen garanderen (7% minder dan in 2015)
- zegt 35% de organisatie te hebben ingericht conform belangrijke richtlijn voor informatiebeveiliging en privacy; NEN 7510 (3% meer dan in 2015)
- heeft 27% een bewustwordingsprogramma informatieveiligheid en privacy voor haar medewerkers
- zegt 27% het afgelopen jaar te maken hebben gehad met privacy-incidenten



3. Het belang van privacy en informatieveiligheid

Er kan veel misgaan, ook bij Emergis

Laptop met gevoelige cliënt gegevens kwijt

WOENSDAG 24 JUNI 2015, 13:56

2015

Beloning voor verloren laptop met gevoelige informatie Emergis



OOST-SOUBURG - Bij de afdeling kinder- en jeugdpsychiatrie van Emergis is in mei een laptop en een harde schijf met gevoelige informatie verdwenen. Op de laptop en harde schijf staat gevoelige informatie over een aantal cliënten.



Overige privacy incidenten binnen Emergis

1. Mail en/of brief met privacygevoelige informatie verstuurd naar verkeerde persoon
2. Niet actuele verzendlijsten gebruikt waardoor medewerkers gegevens hebben ontvangen die niet voor hen bestemd zijn
3. Documenten gevonden achter de printer



Het belang van Informatiebeveiliging en privacybescherming



Het belang van Informatiebeveiliging en privacybescherming

1. Kwaliteit van de zorg; belang van de cliënt staat centraal



Het belang van Informatiebeveiliging en privacybescherming

1. Kwaliteit van de zorg
- 2. Continuïteit van de zorg**



Het belang van Informatiebeveiliging en privacybescherming



Het belang van Informatiebeveiliging en privacybescherming

1. Kwaliteit van de zorg
2. Continuïteit van de zorg
- 3. Beroepsprofessionaliteit/Governancecode
Zorg**



Het belang van Informatiebeveiliging en privacybescherming

1. Kwaliteit van de zorg
2. Continuïteit van de zorg
3. Beroepsprofessionaliteit
- 4. Voldoen aan geldende wet- en regelgeving**



4. Aanpak van informatiebeveiliging en privacybeleid binnen Emergis



Informatiebeveiliging en privacybeleid kent 3 belangrijke aspecten

1. 80% mensenwerk, vraagt om bewustwording
2. Gebouw en ICT infrastructuur vraagt om techniek beveiliging
3. Complexiteit vraagt om beleid en organisatie



Uitgangspunten binnen Emergis m.b.t. Informatiebeveiliging en privacybeleid

- We zijn met z'n allen verantwoordelijk; medewerkers, management en directie/RvB
- Beheersmaatregelen toepassen daar waar mogelijk + bewustwording medewerkers van hun eigen verantwoordelijkheid
- We werken met medische gegevens; bijzondere gegevens waarvoor beroepsgeheim geldt



Aanpak van informatiebeveiliging en privacybeleid binnen Emergis

Beleid en organisatie (1)

- Geïnvesteed in eigen deskundigheid binnen de organisatie:
 - Een werkgroep informatiebeveiliging
 - Een Platform datalekken
 - Functionaris informatiebeveiliging
 - Functionaris Gegevensbescherming



Aanpak van informatiebeveiliging en privacybeleid binnen Emergis

Beleid en organisatie (2)

- Een risico analyse / O-meting uitgevoerd
- Informatiebeveiligingsbeleid en een privacybeleid opgesteld met o.a.:
 - ‘Clear Screen’ en Clean desk’ beleid
 - Wachtwoordenbeleid
 - Digitale meldplicht voor medewerkers van privacy incidenten richting Platform Datalekken



Aanpak van informatiebeveiliging en privacybeleid binnen Emergis

Beleid en organisatie (3)

- Platform Datalekken bestaat uit; bestuurder, geneesheer directeur, functionaris informatiebeveiliging, functionaris gegevensbescherming + externe juridische ondersteuning
- Binnen wettelijke eis van 72 uur worden incidenten gemeld aan Autoriteit Persoonsgegevens
- Meldcultuur ontstaan; bij de geringste twijfel, altijd melden



Aanpak van informatiebeveiliging en privacybeleid binnen Emergis

Beleid en organisatie (4)

- Continuïteitsbeleid
- Werken aan certificering NEN 7510 en ISO27001
- Werken aan implementatie van een Information Security Management System (ISMS) als integraal onderdeel van het totale kwaliteitssysteem



Aanpak van informatiebeveiliging en privacybeleid binnen Emergis

Beleid en organisatie (5)

- Specifiek voor privacybeleid is er dit jaar en komende jaren nog aandacht nodig voor de volgende zaken:
 - Toegang tot Elektronisch Patiënten Dossier (EPD) op basis van afdeling inperken tot relatie behandelaar – cliënt
 - Privacy boekhouding (conform 'best practices' van GGZ Nederland)
 - Privacy Impact Analyses op bestaande en nieuwe kritische processen
 - Bewerkersovereenkomsten met leveranciers die in aanraking komen met privacy gevoelige informatie



Aanpak van informatiebeveiliging en privacybeleid binnen Emergis

Techniek en beleid

- Autorisatie; wie heeft toegang tot welke gegevens en op basis van welke rol?
- Er zijn penetratietesten uitgevoerd om de IT-systemen te testen
- Naast antivirus scanners ook een 24/7 vulnerability scanner actief
- Versleutelde mailverbinding via Zorgmail met TLS (wordt verder uitgebouwd)

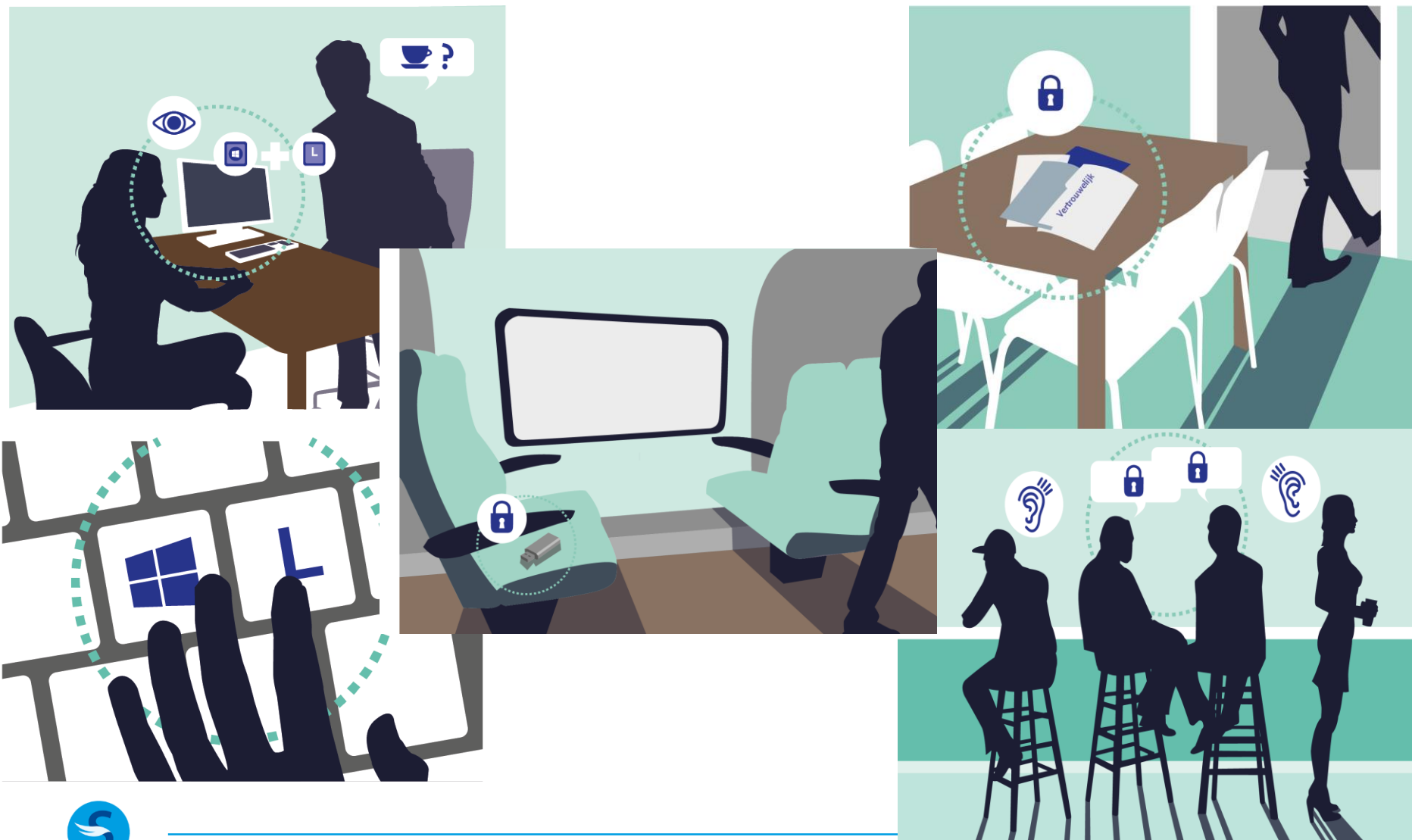


Aanpak van informatiebeveiliging en privacybeleid binnen Emergis

Bewustwording (1)

- 0-meting onder medewerkers; enquête die bewustwording meet
- Een communicatieplan opgesteld en uitgevoerd met volgende elementen:
 - workshops Managers – train the trainer en zegt het voort
 - afdelingsoverleggen bezoeken, in gesprek gaan met medewerkers op de werkvloer
 - aandacht in personeelsblad
 - aandacht op Intranet met Top 12 adviezen, bijv. Windows +L om scherm te vergrendelen
 - ontwikkelen E-learning Informatiebeveiliging en privacy
 - posters met onderwerpen worden op diverse locaties geplaatst





Aanpak van informatiebeveiliging en privacybeleid binnen Emergis

Bewustwording (2)

- Medewerkers worden gevraagd alle informatiebeveiligingsincidenten digitaal te melden om zo ook verder te kunnen verbeteren als organisatie
- Schoonmakers laten info kaartjes achter op bureaus waar nog papieren/documenten zijn blijven liggen

Nog te doen:

- Trainen van medewerkers als interne auditor m.b.t. informatiebeveiliging
- Aansluiten bij landelijke bewustwordingscampagne privacybescherming en informatieveiligheid van de NVZ en GGZ Nederland van 2 t/m 13 oktober 2017



Aanpak van informatiebeveiliging en privacybeleid binnen Emergis

Stand van Zaken inrichten privacybeleid conform Europese Privacy Verordening

50% gerealiseerd voor wat nodig is om op 25 mei 2018 volledig te voldoen aan Europese Privacy Verordening



Waar lopen we tegen aan; obstakels en dilemma's

- Het spanningsveld in de afweging tussen individuele en organisatie verantwoordelijkheid m.b.t. delen/uitwisselen van informatie
- De juiste balans tussen zo goed mogelijke zorg verlenen in belang van de cliënt en de eisen in kader van privacybescherming/informatiebeveiliging
- Hoe maak je medewerkers blijvend bewust van hun verantwoordelijkheid voor privacy en informatiebeveiliging
- De keten van informatiebeveiliging en privacybescherming is zo sterk als de zwakste schakel. Je hebt met veel partijen buiten je organisatie te maken waar je geen controle over hebt.



Waar lopen we tegen aan; obstakels en dilemma's

- Lastig en ingewikkeld om in kader van het ISMS, zo volledig mogelijk te zijn m.b.t. alle processen met relevante zaken voor informatiebeveiliging en privacy
- Het uitvoering geven aan de beheersmaatregelen, waarbij niet altijd direct duidelijk is wie probleem/proces eigenaar is
- Bij sommige partijen kan het lastig zijn om snel tot een bewerkersovereenkomst te komen omdat men grotere aansprakelijkheid vreest



5. Enkele tips en adviezen



Enkele tips en adviezen



1. Begin op tijd
2. Creëer draagvlak voor beleid, te beginnen bij RvB, directie, MT
3. Geef veel aandacht aan bewustwording
4. Maak een goede inventarisatie van processen, middelen en informatie die van belang zijn in kader van privacy en informatiebeveiliging
5. Werk met een Plan van Aanpak dat rekening houdt met mogelijkheden en draagkracht van de organisatie
6. Maak gebruik van beschikbare materiaal bij GGZ Nederland en van 'best practices' bij andere zorgverleners en wissel ervaringen uit met collega's zoals binnen de expertgroep van een EPD-leverancier



Informatieveiligheid is een rijdende trein waar elke keer weer een wagon bij komt



Vragen





Swinth IvO-Partners

Uw kennispartner voor informatieveiligheid en privacy beleid

Sumatrastraat 233
2585 CR Den Haag
+31(0)70 7200960
info@ivo-partners.nl
www.ivo-partners.nl