HACKING AURIS

Event PO-raad
13 september 2024

Tijs van der Wielen
Raad van Bestuur

AURIS
KONINKLIJKE AURIS GROEP

KONINKLIJKE AURIS GROEP

De Koninklijke Auris Groep is een **zorg- en onderwijsorganisatie** (cluster 2) voor kinderen en volwassenen die **ernstige problemen** hebben met **horen, spreken of hun taalontwikkeling**. Auris bestaat uit scholen voor (voortgezet) speciaal onderwijs, ambulante diensten, audiologische centra en zorglocaties. Auris zorgt voor passend onderwijs en begeleidt professionals door advies te geven en scholing bijvoorbeeld vanuit het Auris Cursuscentrum. In 2018 werd Auris Zorg erkend als expertiseorganisatie Zintuiglijk Gehandicapten. Voor Auris werken **2000 medewerkers** en Auris heeft een jaarlijkse omzet van EUR 150 mio. Het werkgebied van Auris is Midden Nederland, Zuid-Holland, Zeeland, Noord-Brabant, Haarlem en Leiden en omgeving.

AURIS
KONINKLIJKE AURIS GROEP

400.000 euro boete

Transavia krijgt boete om slechte beveiliging, hacker kon bij data van 25 miljoen mensen

NOS

'Hackers eisen 50 miljoen dollar van Mediamarkt'

De hackers die Mediamarkt hebben aangevallen, eisen 50 miljoen dollar van de elektronicaketen. Dat meldt RTL Nieuws na onderzoek.

6 dagen geleden

Middelbare school betaalt losgeld na cyberaanval: 'Examens in gevaar'

Losgeld gevraagd

Hogeschool betaalt hacker niet, honderdduizenden privégegevens op straat

Cliëntgegevens gestolen bij hackaanval op zorgorganisatie Auris

RTL Nieuws

Grote hack bij ROC Mondriaan: computers plat en bestanden ...

Onderwijsinstelling ROC Mondriaan in Den Haag is afgelopen weekend gehackt door criminelen. De computers liggen plat en medewerkers en...

23 aug. 2021

DE HACK

- Op woensdag 29 september 2021 waren **alle bestanden op het netwerk versleuteld**
- De organisatie lag **digitaal** van het ene moment op het andere **plat**
- Direct een **intern crisisteam** geïnstalleerd met RvB, ICT, FG, CISO en Communicatie
- Direct een **extern crisisteam** ingericht met Auris, ICT dienstverlener en **specialistisch ICT security bedrijf**
- **Analyse** van de problematiek (complex), start **forensisch onderzoek**
- **Onderhandeling** met hackersgroep via specialistisch ICT security bedrijf
- Direct **aangifte politie** en **voorlopige melding Autoriteit Persoonsgegevens**
- Plan: **Stap voor stap weer online** in vier weken, incl. screening van alle devices in de heropbouw

AURIS
KONINKLIJKE AURIS GROEP

FORENSISCH ONDERZOEK

Uit **forensisch onderzoek** bleek:

- De hacker was al **eerder die maand binnen** gekomen, maar **onopgemerkt** gebleven
- **Later** die maand is de **aanvaller** binnengekomen en heeft allerlei software geïnstalleerd, **data gestolen** via een onbekende dropbox en vervolgend de **encryptie software** geactiveerd
- Het betrof alleen de **netwerkschijven**, de **cloud** (zoals MS Office en Parnasys) was **niet besmet**
- **Backups** waren **niet versleuteld**, dus dataloss ogenschijnlijk niet groot
- De hackersgroep komt uit Rusland en vroeg **losgeld** voor encryptiesleutel en het niet **verkopen** van de **gestolen data**

AURIS
KONINKLIJKE AURIS GROEP

DE CRISIS

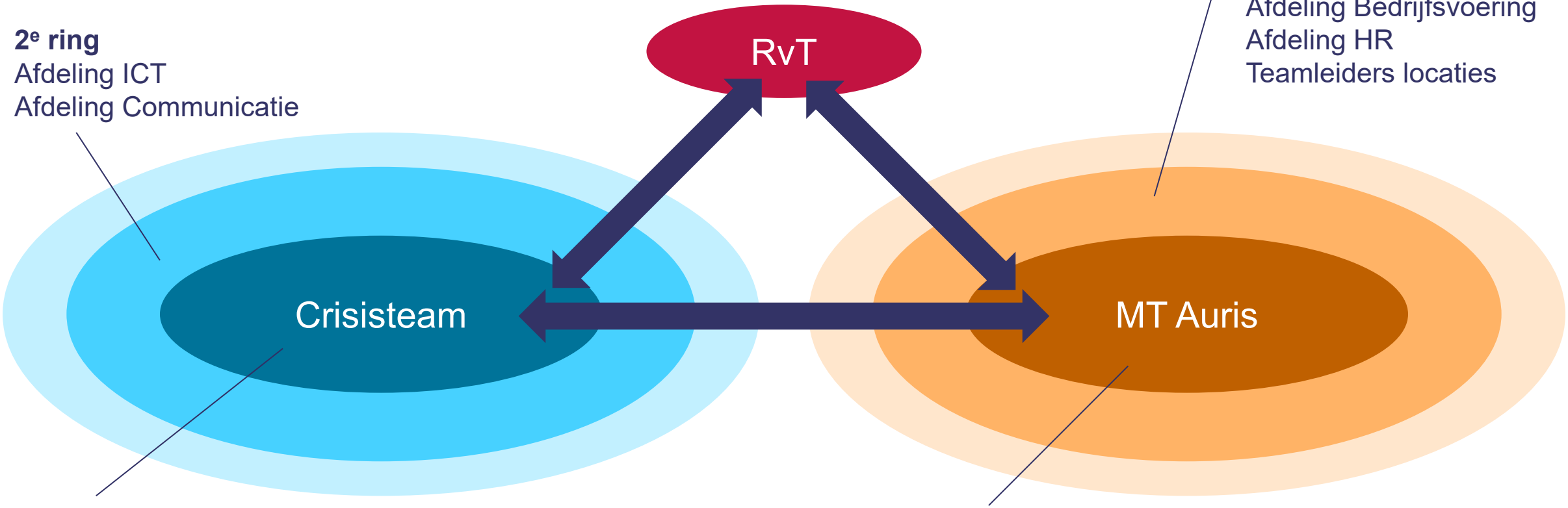
AURIS
KONINKLIJKE AURIS GROEP

AURIS.NL

HET INTERN CRISISTEAM

2e ring
Afdeling ICT
Afdeling Communicatie

2e ring
Afdeling Bedrijfsvoering
Afdeling HR
Teamleiders locaties



Crisisteam (1e ring)
1x RvB (vz crisisteam)
1x FG
1x CISO
3x ICT (Hoofd ICT & verschillende expertises)
1x Communicatie
1x Ondersteuner (Notulen, Logboek!, etc.)

MT (1e ring)
1x RvB (vz)
6x Regiodirectie
3x Stafhoofden
1x Concern controler
1x Communicatie
1x Ondersteuner

AURIS
KONINKLIJKE AURIS GROEP

DE CRISIS

- **Crisisteam** handelt de **crisis**, **MT** Auris handelt de **organisatie** (going concern)
  - **RvB** heeft de **leiding** over beide gremia en **stuurt** deze ook **zelf aan** vanuit ieder zijn eigen team
  - RvB onderling veel afstemming, RvB Crisisteam schakelt met Voorzitter RvT
  - 1e ring stuurt de 2e ring aan, 2e ring stuurt de 3e ring aan
  - Aantal deelnemers **1e ring beperkt!**
- Planmatig ingezet op **communicatie** via een tweetal apps (intranet en email plat)
  - Calamiteiten **appgroepen** beschikbaar
  - Persbericht / statement
- **Crisisplannen** niet beschikbaar, stonden online
  - Zorg voor een **hardcopy** in de kast
  - Zorg dat je ook dergelijke incidenten ook **oefent** (cf. IPB normenkader)
- MT: direct een **knelpuntenanalyse kritische processen** opgesteld met consequenties, risico's en **prioritering** (bijv. onderwijs, zorgverlening / diagnostiek, maar ook bijv. salarisbetaling)

AURIS
KONINKLIJKE AURIS GROEP

BESTUURLIJKE AFWEGINGEN

- Gaan we voor **snelheid of veiligheid** in de heropbouw van IT?
- Wat is **de impact** van de hack en de gesloten data? Op de organisatie, op de cliënten / ouders en leerlingen, op de medewerker? Lopen we **imago-schade** op?
- Gaan we **wel of niet betalen**? In afstemming met de RvT niet betaald
- Hoe kijkt de **medewerker** hier tegenaan als het gaat over **haar gegevens**?
- Wat **communiceren** we hier intern en extern over? Zoeken we **actief de media**?
- Hoe blijven we **uit de juridische modus** (schuldvraag) met de IT Dienstverlener zodat het herstel niet vertraagd?
- Welke **systemen en applicaties** brengen we **als eerste** weer **online**?
- Welke **processen** zijn kritisch in de bedrijfsvoering en krijgen **voorrang**?
- Wat is de directe en indirecte **financiële schade** door inhuur specialistisch ICT security bedrijf, omzetverlies zorg, vertraging allerlei processen, etc. Wie gaat dit betalen?
- …

AURIS
KONINKLIJKE AURIS GROEP

LESSONS LEARNED / VOORBEREIDING

AURIS
KONINKLIJKE AURIS GROEP

AURIS.NL

LESSONS LEARNED

- Auris heeft een **duidelijke strategie** (GO.01 & GO.02) met een **meerjaren routemap** (GO.03) naar een hoger level van ICT security, **snel genoeg?**
- Auris was goed beveiligd, maar een **zwakke plek** is zo gecreëerd en gevonden
- Regelmatig **PEN testen** uitvoeren / **NEN 7510** audit en verankeren in de **P&C cyclus** (GO.05)
- Er was aandacht voor ICT security binnen de RvB, **sturing** had achteraf **stelliger gekund**
- ICT was **te dienstverlenend** (of de lijn te dominant), pragmatiek voor security
- Het **budget** voor ICT moet de komende tijd nog verder omhoog (Hoe gaan we dit de komende jaren financieren?)
- **Schade relatief beperkt** door al veel te hebben **geïnvesteerd** in **ICT en cloud-applicaties**
- Opnieuw bekijken of een **verzekering rendabel** is, twee jaar geleden niet
- Gebruik het **Normenkader IBP**!

Het kan iedereen overkomen en het is geen “ver van mijn bed show” meer!

AURIS
KONINKLIJKE AURIS GROEP

VOORBEREIDING

Normenkader IBP!

De domeinen van informatiebeveiliging:

- Domein 1: Bestuur
- Domein 2: Organisatie
- Domein 3: Risicomanagement
- Domein 4: Personeelsbeheer
- Domein 5: Configuratiemanagement
- Domein 6: Incident- en problemmanagement
- Domein 7: Changemanagement
- Domein 8: Systeemontwikkeling
- Domein 9: Datamanagement
- Domein 10: Identity- en accessmanagement
- Domein 11: Securitymanagement
- Domein 12: Fysieke beveiliging
- Domein 13: It-operatie
- Domein 14: Bedrijfscontinuïteitsmanagement
- Domein 15: Ketenbeheer

AURIS
KONINKLIJKE AURIS GROEP

VRAGEN?

AURIS
KONINKLIJKE AURIS GROEP

AURIS.NL