


Casus Hof van Twente

Kees Hintzbergen - IBD



Agenda

- Introductie
 - Hoe zag het eruit voor december 2020?
 - Wat is er gebeurd?
 - Dilemma's
 - Hoe zit dat bij jou?
 - Tips aan elkaar
- 

Reflectie op verhaal Dennis Lacroix

Reactie in de chat:


- Wat viel je op aan de presentatie van Dennis?
- Wat was de reactie binnen jullie gemeente toen jullie hiervan hoorden ?

Esther Apperloo de CISO van HvT



Hoe zag het er in Hof van Twente uit voor december 2020?


Eigenlijk alles goed op orde:

- ENSIA groen
 - Pentest uitgevoerd
 - Zorgvuldige overweging over beheer IT
 - I&A visie
 - BCM plan vastgesteld
- 

Opvallend

- Vooraf:
 - Op 9 november 2020 toegang aanvallers via RDP-poort
 - Tussen 24 november en 1 december 323.000 inlogpogingen tot de log vol was
 - Vorige week nog op een openbare lijst met gecompromitteerde RDP-accounts
 - Scope pentest niet groot genoeg
 - Back-up versleuteld

Dilemma's

- Toch maar even over losgeldbetalingen
 - Werk, vertrouwen, garantie
 - Betrekken veiligheidsregio
 - Incidentmanagers, crisisbeheersing
 - Data recovery/opnieuw opbouwen
- 

Hoe zit het bij jou?

- Heb je communicatie van de IBD gezien aangaande HvT?
- ENSIA als sturingsinstrument
- Risico's in beeld
- BCM-plan
- Backup en Restore
- Incidentmanagementproces
- Wie heb je direct aan tafel bij een crisis?



Tips aan elkaar

- Welke tip heeft u voor de andere aanwezigen?

Tips uit vorige sessies

- Ga met de lessen uit hof van Twente even langs bij je systeembeheerder/Hoofd ICT/CISO
- Zorg dat de Ensia rapportage een eerlijk beeld geeft
- Gebruik het moment van de Ensia rapportage om management en bestuur te wijzen op de risico's door (nog) niet genomen maatregelen
- IBD gaat bestuurlijke lessen binnenkort verspreiden onder Gemeentesecretarissen, gebruik deze om aandacht te krijgen op het onderwerp en controleer of er nieuwe IB-plannen zijn.

Lessen uit hof van Twente

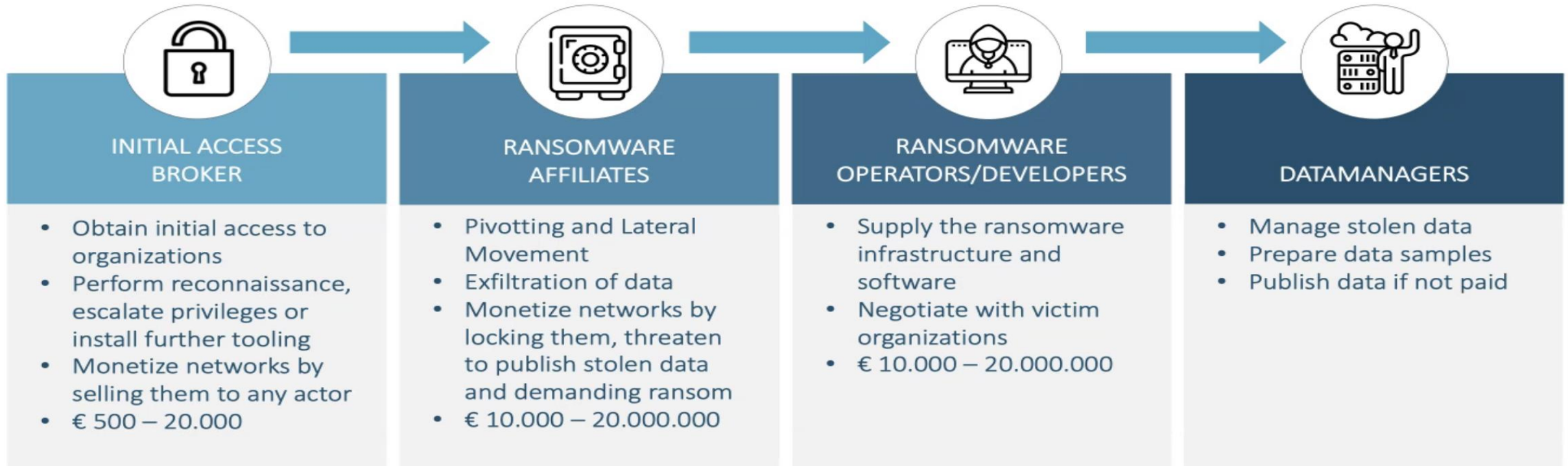
- Preventie is niet alles
- Betrek:
 - de IBD vroegtijdig (wees open)
 - gespecialiseerde hulp inhuren
 - collega's van andere gemeenten
- Het gaat een keer gebeuren, zorg dat je er klaar voor bent
- BCM
 - Beleid: welke processen eerst> door MT laten vaststellen
 - Plan: wat is daarvoor nodig en hoe regel ik dat, briefje meterkast
 - Oefenen
- Zorg ook voor vervanging Ciso

Vraag aan u ter overweging

Wetende dat u morgen slachtoffer wordt van een ransomware aanval, wat zou u vandaag dan doen?

Ransomware as a service

RANSOMWARE AS A SERVICE - SUPPLY CHAIN



INFORMATIE
BEVEILIGINGS
DIENST

Vragen?

