Reactie vanuit MKB Cybercampus[1]

Henk van Ee (8 februari 2020)

Inleiding

Het discussiestuk “een IT Deltaplan voor de overheid” is de directe aanleiding voor deze notitie. Hieronder wordt specifiek ingegaan op de uitdagingen waarmee de (digitale) overheid zich steeds meer geconfronteerd zal zien vanuit het perspectief van cybersafety. De relevantie moge ook duidelijk zijn getuige de vele cyber gerelateerde incidenten waarbij zowel overheden, organisaties als bedrijven slachtoffer werden van gedigitaliseerde criminaliteit en cybercriminaliteit.
Wat is de impact hiervan op de uitdagingen bij de overheid en welke aanbevelingen volgen hier logischerwijs uit?

De uitdagingen in het cyberdomein

Ook de ICT binnen de overheid is kwetsbaar gebleken voor cyberaanvallen en die kwetsbaarheid zal toenemen als ook gelet wordt op het steeds “slimmer” worden van cyberaanvallen. Steeds gerichter en steeds meer geautomatiseerd worden aanvallen uitgevoerd waarbij de beheersmaatregelen om deze aanvallen te voorkomen, signaleren, verstoren en de impact ervan te beperken, om steeds grotere investeringen vragen.
De aanvallen kunnen heel divers zijn en worden zoals gezegd steeds gerichter waarbij geldt dat cybercriminelen in het voordeel zijn: er hoeft maar 1 medewerker op een linkje te klikken, er hoeft maar 1 server niet van de nieuwste beveiligingssoftware voorzien te zijn of 1 toeleverancier hoeft maar makkelijk hackbaar te zijn zodat de bedreiging via regulier ogende processen via de keten binnen komt.

Deze ketenafhankelijkheid wordt een steeds grotere uitdaging: waar grotere partijen in de kritieke infrastructuur steeds geavanceerde beheersmaatregelen genomen hebben, is de kans dat er een verschuiving van de dreiging en aanvalsvector naar ketenpartners plaatsvindt, relevant. Hoe is bijvoorbeeld de IT-security geregeld bij MKB-bedrijven die onderhoud uitvoeren op technische installaties zoals sluizen, waterwerken, brandinstallaties?

Naast deze uitdaging is de uitdaging van zowel de complexiteit van de ICT infrastructuur in relatie tot de factor mens relevant. Zeker gezien het tekort aan technische specialisten, is het voor cybercriminelen interessant om in de ICT beheersorganisatie bij de overheid zelf maar ook bij toeleveranciers te infiltreren en zo relatief eenvoudig toegang te krijgen tot de zogenaamde high privilege accounts en waarmee veel schade aangericht kan worden.
Deze infiltratie is evident bij dit soort functies maar moet in een breder perspectief gezien worden en kan ook in andere processen/afdelingen plaatsvinden waardoor ondermijningsactiviteiten uitgevoerd kunnen worden en lang “onder de radar” kunnen blijven. Denk hierbij aan functies als functioneel beheerders, informatiemanagers maar ook de rol van CISO is natuurlijk interessant.

---

1 https://mkbcybercampus.nl/

Een andere uitdaging ligt in de opkomende wereld van Internet of Things en de wijze waarop cybersafety een aspect is bij installatie, onderhoud en toepassing hiervan. Het werkveld van bijvoorbeeld installatiebedrijven zoekt inmiddels personeel dat in staat is zowel de basiselectronica te begrijpen en toe te passen maar ook verstand heeft van ICT en kan programmeren. Een groeiende uitdaging.

Een laatste uitdaging in dit niet uitputtende overzicht is dat steeds meer processen meer digitale koppelingen in zich hebben en organisaties/instanties/afdelingen meer digitaal verbonden zijn dan beseft wordt met alle risico's van dien. Dat geldt ook voor de overheid zelf: is voldoende in beeld welke andere processen "geraakt" worden als een proces in een ander domein niet beschikbaar is door bijvoorbeeld een cyberaanval? Is nog voldoende in beeld waar overal gegevens gebruikt en toegepast worden?

Aanbevelingen

Wat betekenen deze aanbevelingen concreet naast de aanbevelingen die al gedaan worden in het Deltaplan? Zonder de illusie te hebben uitputtend te zijn hierbij een aantal aanbevelingen om de uitdagingen zoals geschetst hiervoor te adresseren:

1. Neem bij ICT-projecten ook expliciet informatiebeveiliging op met specifieke focus op:
    a. Detectiemaatregelen;
    b. Inzicht in ketenprocessen: welke digitale koppelingen ontstaan en welke impact heeft dat?
    c. Back up scenario's: wat en hoe is er geregeld ook offline als het proces dat digitaal ondersteund wordt, uit mocht vallen?
2. Voer een risicoscan uit:
    a. Hoe is het gesteld met de factor mens in de breedste zins des woords: wie heeft waar toegang toe zowel binnen als buiten de overheid met specifieke aandacht voor de zogenaamde high privilege accounts en hoe vindt monitoring op deze kwetsbare groep personeel plaats en hoe worden ze weerbaar gemaakt voor social engineering/omkoping?
    b. Welke digitale koppelingen in ketenprocessen bestaan er inmiddels en welke kwetsbaarheden blijken daar uit?
    c. Wat is de staat van informatiebeveiliging bij toeleveranciers in de keten van de overheid en neem daar maatregelen op?
    d. Kwetsbaarheden in de keten: voer gerichte security testen uit op kwetsbaarheden in de keten!
3. Tref meer voorbereidingen in het offline domein als kritieke processen uitvallen als gevolg van uitvallen van digitale processen. Ontwikkel vooral integraal en met ketenpartners scenario's zodat de weerbaarheid omhoog gaat en de digitale afhankelijkheid minder groot wordt. Naast ontwikkelen van scenario's zal gericht oefenen hiervan ook essentieel zijn.
4. Pas versneld het onderwijsaanbod aan op de nieuwe uitdagingen
   In dit verband is specifiek IoT interessant: hoe zorgen we er voor dat vakopleidingen meer geïntegreerd worden zodat de "digitale loodgieter" van vandaag de dag behalve met de steeksleutel om kan gaan, ook zijn of haar weg weet in programmeren.