digital trust center.

Cyberoefengame 'Ransomware'

Spelhandleiding

Ontwikkeld in samenwerking met: ARDA

Inhoud

1. INLEIDING

1.1 Waarom deze game?

Het Digital Trust Center wil het bedrijfsleven in Nederland cyberweerbaar maken. Weerbaarheid betekent dat je ook adequaat reageert in crisissituaties. Dit kun je oefenen.

We zijn steeds afhankelijker van ICT als het gaat om onze bedrijfsvoering en productie. Een cyberaanval op digitale processen kan aanzienlijke gevolgen hebben. Om onze veerkracht te versterken, is het zinvol om de reactie op digitale dreigingen te oefenen. Dat kan heel goed in de vorm van een serious game.

Dit document is een spelhandleiding voor de cyberoefengame ‘ransomware’. Dit document is bedoeld voor de spelleiders die deze game binnen hun organisatie willen spelen. Het geeft je handige tips voor tijdens het spelen.

1.2 Doelstellingen van het project

1. Kennisopbouw: Je doet kennis op op het gebied van cybersecurity, crisisscenario's, en crisismanagement.
2. Samenwerking: Met behulp van de serious game leren medewerkers de verschillende rollen in de organisatie kennen, leren ze van elkaar en ontstaan er korte lijntjes.
3. Bewustwording: De medewerkers leren wat er te doen is in het geval van een crisissituatie.
4. Incident response: Is je eigen bedrijf of organisatie voorbereid om adequaat te reageren op een ernstige cybercrisis? Biedt je incident response plan voldoende houvast?

1.3 Metafoor: Waterbedrijf Alisson

Voor de game is er gekozen voor een fictief waterbedrijf in Nederland met de naam Alisson. Het bedrijf heeft 450 medewerkers en krijgt te maken met een ransomware-aanval. Als speler van de game zie je hoe dit cyberincidenten zich manifesteert. Maak kennis met het crisisteam van Alisson.

Mirjam
Voorzitter crisisteam

Brian
IT-manager

Nanette
Hoofd communicatie

Stan
Manager productie

De informatie uit de vorige paragrafen wordt ook aan de deelnemers verteld in de eerste video tijdens het spel.

2. JOUW ROL ALS SPELLEIDER

Bekijk de video

Dag spelleider, wat leuk dat je hier bent en spelleider wilt zijn voor deze serious game. Je speelt een belangrijke rol in deze serious game. Jouw rol is om de deelnemers te ondersteunen en eventueel toelichting te geven over de situatie bij Alisson. Je mag de deelnemers uitdagen kritische vragen te stellen over de aanpak bij de eigen organisatie en ze te stimuleren met elkaar te discussiëren over alternatieve aanpakken. Als spelleider is jouw toverwoord: waarom?

Deelnemers aan deze game vertalen de situatie die ze zien bij Allison naar hun eigen bedrijf, en krijgen daardoor inzichten in hoe dingen bij het eigen bedrijf al dan niet geregeld zijn, en wat ze daarvan wel of niet weten. Als spelleider stimuleer je dit proces.

De game bestaat uit filmscènes, afgewisseld met kennisvragen en momenten voor discussie. Vragen die bijvoorbeeld gesteld worden zijn:

- Stel dat zoiets bij jullie bedrijf voorkomt. Wie zou hier verantwoordelijk voor zijn? of
- Zouden jullie in deze situatie opschalen?

Let op, deze game is bedoeld voor personen met verschillende achtergronden en kennisniveaus. Het streven is niet 100% technische accuratie. Om de scenario's interessant en behapbaar te maken zijn ze hier en daar verkort; in het echt zou een gebeurtenis langer duren of meer aspecten behandelen.

Met jouw ondersteuning kan de kennis rondom de aanpak van een cybercalamiteit worden verbeterd, zodat - als deze zich in het echt voordoet - deelnemers beter weten hoe te handelen en welke invloed hun acties kunnen hebben op het verloop van de behandeling van de calamiteit. Jouw rol is dus zeer belangrijk tijdens het spelen van deze cyberoefening. Succes en veel plezier!

2.1 Tips voor het spelen (in het geval van online spelen)

- Zorg dat spelers niet via een Citrix-verbinding of met scherm delen spelen. Dat geeft namelijk slecht geluid en schokkende beelden.
- Het spel spelen door het scherm te delen werkt niet. Dan is er geen geluid. Laat iedereen op zijn eigen apparaat naar de link gaan.
- Laat deelnemers deelnemen via computer of iPad met twee schermen open. Eén met het spel en één met Teams. De spelleider/begeleider geeft dan aan wanneer er naar het spel gekeken moet worden en wanneer iedereen weer in de Teams-omgeving moet terugkeren om daar antwoorden op de vragen te geven en/of te gaan discussiëren.

2. JOUW ROL ALS SPELLEIDER

2.2 Discussie laten ontstaan

Als tijdens de beantwoording van de vraag blijkt dat de deelnemers heel andere antwoorden zouden willen geven, daag ze dan uit dit te doen en vraag vooral ook: waarom. Waarom dit 'eigen' antwoord en niet eentje vanuit de geboden keuzes?

Tijdens discussiemomenten is het goed om even te reflecteren op wat er gebeurde in het spel versus de realiteit. Motiveer de spelers bijvoorbeeld door middel van de bijgeleverde feedback om de situatie van een andere kant te bekijken.

Mocht het even stilvallen dan kun je bijvoorbeeld de volgende vragen stellen:

- Wat is je primaire gedachte bij deze scène?
- Hoe had jij (specifiek persoon) dit aangepakt?
- Heb je eerder een soortgelijk incident meegemaakt?
- Waarom denk je dat Allison deze keuzes heeft gemaakt?

Spreek soms ook direct iemand aan bij naam. Laat iedereen even aan de beurt komen om reactie op elkaar te geven.

3. BENODIGDHEDEN OM TE SPELEN

3.1 Duur van de game

Neem voor iedere game sessie ongeveer anderhalf uur de tijd.

- Een kwartier om op te zetten.
- Drie kwartier om te spelen.
- Een half uur nabespreking.

3.2 Deelnemers

Je kunt de oefening doen met 2 tot 7 deelnemers. De oefening is bij uitstek geschikt voor medewerkers die in de eigen organisatie een rol hebben bij het beheersen van crisissituaties, maar ook medewerkers zonder deze betrokkenheid, hebben baat bij de oefening. Het geeft een waardevolle bewustwording van de gevolgen van digitaal onveilig gedrag.

Je kunt deze oefening ook doen met andere bedrijven in je keten als aanzet tot het inventariseren van ketenrisico's.

3.3 Benodigdheden fysieke game sessie

- Een goede internetverbinding.
- Een ruimte waar je gezamenlijk met de groep kunt zitten en overleggen.
- Een centraal scherm waarop het spel te spelen is met speakers voor de video's
- De game flow voor het scenario wat je gaat spelen met feedback tips.

4. HOE ZET JE EEN DIGITALE SESSIE OP

4.1 Bereid de spelers goed voor

Om spelers goed voor te bereiden, breng je ze op de hoogte van wat er komen gaat. Gebruik hiervoor bijvoorbeeld deze template e-mail:

Wat zou jij doen? Uitnodiging deelname serious game

Kruip met de kennis die je hebt van je eigen bedrijf in de huid van fictief waterbedrijf Allison. Aan de hand van een filmfragmenten word je meegenomen in een crisissituatie na een ransomware-aanval. Je mag meedenken hoe het crisisteam dit moet oplosssen.

We gaan cyberoefenen aan de hand van een serious game. Een serious game is een spel dat ontwikkeld is met een doel om je niet alleen te entertainen, maar ook om je iets te leren door het je te laten ervaren.

Meer verklappen we niet voor nu. Een week van te voren ontvang je nadere informatie.

Bekijk de teaser

Reminder:

Binnenkort spelen we samen de serious game Ransomware. We zullen in totaal ongeveer 1,5 uur bezig zijn.

We spelen in een digitale setting dus we bellen eerst in via Teams / Zoom / overig. Het spel bevat video en audio elementen, speel daarom bij voorkeur op een laptop of desktop met een koptelefoon op.

4.2 Sessie opzetten spelleider

Tijdens de digitale sessie heb je het volgende nodig:

- Geprinte handleiding/flow van het spel.
- Een groot scherm met geluid en internet.
- Optioneel: het incident response plan of bellijst van je eigen organisatie

5. GAMEFLOW Ransomware

Dit scenario heeft als onderwerp ransomware. Ransomware is een van de meest drastische hacks die een bedrijf kan overkomen, er is voor criminelen veel geld mee te verdienen en het lijkt daarom steeds vaker voor te komen. Bij een ransomware aanval weten hackers systemen en data van een bedrijf over te nemen en te versleutelen. Het bedrijf krijgt alleen de toegang terug als ze losgeld betalen.

In dit scenario wordt een leverancier van Alisson - Castra - geraakt met ransomware. Hierdoor komen er verschillende processen van Alisson stil te liggen. Het crisisteam komt voor een moeilijke beslissing te staan: betalen of opnieuw opbouwen.

Dit scenario bestaat uit:

- 9 scenes
- 8 multiple choice vragen
- 5 discussiepunten

Start de game

5. GAMEFLOW CASTRA

Welkom videopresentator

Scene 1: De kwetsbaarheid komt naar voren

Vraag 1: Reageerde de medewerker goed op dit bericht? Hoe zouden jullie gereageerd hebben? Kan dit in jullie bedrijf voorkomen? Wat zijn hiervoor de procedures?

Hint: De medewerker had het bericht serieuzer moeten nemen en naar de juiste persoon of afdeling moeten doorsturen. In veel gevallen is dit de IT-servicedesk of de (C)ISO. Is bij jullie bedrijf iedereen op de hoogte hoe ze moeten handelen in zo'n geval?

Scene 2: Nanette meldt het bericht bij de servicedesk maar betrekt voor de zekerheid ook Brian.

Vraag 2: In de e-mail die Nanette ontving, vallen de woorden 'ransom' en 'bitcoin' op. Zet ransomware gegevensbestanden en/of IT-systemen op slot?

- **A. Waar**
- B. Niet waar

Bevestig: Het antwoord is 'Waar'. Ransomware versleutelt of vergrendelt gegevens en systemen zodanig dat je er als gebruiker niet meer bij kunt tenzij je de cyberaanvallers ‘ransom’ (losgeld) betaalt. Je krijgt dan een ontsleutelingscode of "decryption key' waarmee je weer toegang tot de bestanden zou moeten krijgen.

Vraag 3: Als er ransomware-software geïnstalleerd wordt, merk je dat meteen!

- A. Waar
- **B. Niet waar**

Bevestig: Het antwoord is 'Niet waar'. Hackers kunnen ransomware installeren en dan vervolgens nog een tijdje in de IT-systemen 'rondhangen’ om zo hun ransomware-aanval goed voor te bereiden. Pas als ze de ransomware activeren, merk je er wat van.

Scene 3: Brian begrijpt de ernst van de situatie beter en maakt zich zorgen.

Vraag 4: Moet Alisson opschalen, op basis van wat jullie net gezien hebben? Geeft het crisiprotocol hier houvast?

Hint: Ja, op basis van de scène en het opschalingsprotocol moet Alisson opschalen. Het is een incident waarbij de normale bedrijfsvoering substantieel is verstoord of dreigt te worden verstoord.

5. GAMEFLOW CASTRA

Scene 4: Het crisisteam komt samen en start de beeldvorming

Vraag 5: Wie van jullie kent de BOB-methode? Werken jullie er zelf ook mee?

Hint: Er zijn 3 fasen: Beeldvorming, Oordeelsvorming en Besluitvorming. Deze fasen onderscheid je strak van elkaar. Je doet eerst de beeldvorming. Pas als die stap helemaal is afgerond stap je over naar de oordeelsvorming en vervolgens besluitvorming. Besluiten leg je altijd vast.

Vraag 6: De kosten van een ransomware-aanval zijn overzichtelijk.

- A. Waar
- **B. Niet waar**

Bevestig: Niet waar. De totale kosten van een ransomware-aanval zijn vaak veel hoger dan alleen het losgeldbedrag. Denk bijvoorbeeld aan de schade die ontstaat doordat je bedrijfsprocessen stil komen te liggen, mogelijke schadeclaims van klanten en onbetaalbare reputatieschade.

Vraag 7: Als je losgeld betaalt, kun je altijd meteen weer verder met je bedrijfsprocessen.

- A. Waar
- **B. Niet waar**

Bevestig: Niet waar. Betaling biedt geen garantie voor teruggave van je gegevens. Soms komen de cybercriminelen terug met hogere eisen. Ze kunnen dreigen om de gestolen gegevens openbaar te maken. Je zult dus altijd aan het herstel van je IT-systemen moeten werken.

Scene 5: Het crisisteam brengt de situatie verder in kaart.

Vraag 8: Stel dat hackers bij de data van Alissons klanten en medewerkers konden. Moet hiervan aangifte gedaan worden bij de Autoriteit Persoonsgegevens?

- **A. Ja**
- B. Nee

Bevestig: Alisson moet een melding maken. Hackers zijn onbevoegden: ze hebben immers geen toestemming gekregen om in de systemen rond te neuzen. Als onbevoegden toegang hebben tot persoonlijke gegevens van bijvoorbeeld medewerkers of klanten, dan moet je hiervan melding doen bij de Autoriteit Persoonsgegevens. Oók als ze geen gegevens lekken of hebben gelekt.

5. GAMEFLOW CASTRA

Vraag 9: Alisson heeft dit datalek op een vrijdag ontdekt. Binnen welk tijdsframe moet er een melding gedaan worden bij de Autoriteit persoonsgegevens voor er een boete gegeven kan worden?

- A. Dezelfde dag als het ontdekken van het lek
- B. Binnen twee werkdagen (uiterlijk dinsdag)
- C. Binnen drie werkdagen (uiterlijk woensdag)
- **D. Binnen drie dagen (uiterlijk maandag)**

Bevestig: Het goede antwoord is "Binnen 3 dagen (uiterlijk maandag)." Je moet een datalek binnen 72 uur na ontdekking melden aan de Autoriteit Persoonsgegevens (AP). Als je te laat bent, moet je dit motiveren. Alleen in uitzonderlijke gevallen accepteert de AP een vertraagde melding na 72 uur.

Bij een complexe inbreuk, zoals digitale hacks of phishing moet je de eerste melding nog steeds binnen 72 uur doen. Bij nieuwe informatie kun je dan een vervolgmelding doen.

Scene 6: Nanette krijgt te horen dat er op X (voormalig Twitter) berichten over de hack worden geplaatst.

Scene 7: Het crisisteam is weer samen en Brian deelt dat er hoogstwaarschijnlijk ook geen back-ups meer beschikbaar zijn. Nanette laat de tweet zien die Jules doorgaf en het team maakt een impactanalyse.

Vraag 10: De ombeschikbaarheid van Castra heeft voor Alisson impact op:

- Verwerken van nota's
- Betalingsherinneringen
- De Mijn Alisson-omgeving die zonder koppeling iet volledig operationeel is
- De beschikbaarheid en integriteit van klant- en werknemersgegevens

Welke gevolgen zou dit kunnen hebben voor de kritieke bedrijfsprocessen van Alisson? Schets samen een scenario.

Hint: Mogelijke scenario's zijn:

- Alisson kan inkomsten mislopen
- Medewerkers kunnen inkomende klantvragen niet beantwoorden
- Gegevens van klanten en medewerkers kunnen gestolen worden

Scene 8: Het crisisteam staat tegenover een moeilijke keuze: betalen of de data en het systeem herbouwen.

Vraag 11: Het inschakelen van een cybersecurity adviseur met ransomware-expertise betekent dat je besluit om te gaan betalen.

- A. Waar
- **B. Niet waar**

5. GAMEFLOW CASTRA

Bevestig: Niet waar. Iemand met ransomware-expertise kan helpen bij het in kaart brengen van je herstelopties. Zijn back-ups nog te herstellen? Zijn er aanwijzigen dat de hackers ook op andere plekken in je netwerk- en IT-systemen zitten? Deze persoon kan ook helpen in het contact met de cybercriminelen als dat nodig is.

Vraag 12: Zouden jullie losgeld betalen? Waarom wel of waarom niet?

Hint: Het advies van de overheid is om geen ransomware te betalen omdat dit het verdienmodel van cybercriminelen in stand houdt en omdat er geen enkele garantie is dat je na betaling weer toegang hebt tot je bestanden of systemen.

Vraag 13: Maak nu een keuze welk einde jullie zouden willen zien:

- A. Alisson betaalt niet aan de hackers en bouwt opnieuw op
- B. Alisson betaalt aan de hackers

Op basis van de keuze van de spelers volgt een bijpassende eindscene met Mirjam.

Afsluitende video

6. NABESPREKING

Aan het eind van iedere game is het een goed idee een korte nabespreking te houden. Verken met de deelnemers wat hun ervaringen, opmerkingen en leerpunten zijn. Stel vragen als:

- Wat vonden jullie van deze specifieke casus?
- Hoe beviel de spelvorm?
- Heb je n.a.v. deze sessie nog vragen die je wilt gaan uitzoeken (en zo ja, wat ga je doen met de antwoorden, hoe deel je die en met wie)?
- Heb je n.a.v. deze sessie nog wensen ten aanzien van een andere oefening of training en zo ja, welke?
- Missen er nu ook nog zaken in onze calamiteitenplannen, handleidingen of afspraken rondom het beheersen van incidenten?
- Tot slot: wat is voor jou de belangrijkste les uit deze oefening?