Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Oefenen baart kunst!

De eerste stappen naar een succesvol oefenprogramma

Inleiding

De medewerkers in jouw organisatie spelen een belangrijke rol in het beheersen van een cyberincident of -crisis. Door regelmatig te oefenen met (fictieve) incidenten bouwen jouw medewerkers ervaring op en kunnen zij effectief handelen. Zonder te oefenen loop je het risico dat je alles op papier tot in de puntjes hebt uitgedacht, maar in praktijk serieus tekort schiet. Maar hoe pak je zo'n oefening effectief aan? Welke oefenvormen zijn er en waar begin je? In deze publicatie lees je meer over het belang van oefenen en krijg je concrete handvatten om een succesvolle oefening te organiseren.

Doelgroep

Ben jij primair betrokken bij de digitale weerbaarheid van jouw organisatie? En wil je weten wat oefenen vor jou kan betekenen en hoe je hier de eerste stappen in kan zetten? Lees dan deze publicatie.

Deze publicatie is tot stand gekomen met bijdragen van

Het Cyberchain Resilience Consortium (CCRC), De Nederlandse Bank (DNB), TCT Rijk, Digital Trust Center, Ministerie van Onderwijs, Cultuur & Wetenschap, Eye security, Esoxit, Het Normo (TCT rijk en het Normo).

Inhoud

Achtergrond: wat is oefenen? 3
1. Schets een oefenplan 3
2. Ontwikkel de oefening en voer deze uit 5
3. Opvolging van de oefening 6

Achtergrond: wat is oefenen?

Oefenen is het *in de praktijk brengen* van wat je hebt geleerd in een gecontroleerde en veilige omgeving. Jij en jouw medewerkers bouwen hiermee ervaring op en kunnen daarmee effectiever handelen tijdens een cyberincident. Door regelmatig te oefenen zorg je er bijvoorbeeld voor dat back-ups snel teruggezet kunnen worden na een ransomware-aanval, er effectief wordt gecommuniceerd bij een datalek en er geen steken vallen bij het managen van een cybercrisis. Er zijn verschillende vormen om te oefenen, zoals:

- **Een tabletop-oefening,** waarbij gespreksdeelnemers gezamenlijk door een scenario lopen en middels een gestructureerde discussie oefenen met hun rol. In een tabletop presenteert de oefenleider stapsgewijs elementen van een scenario en daagt de deelnemers uit hier hun rol in te nemen. Denk aan een fictieve crisis, waarbij het scenario de crisis beschrijft en de informatie waar het crisisteam over beschikt. Na de tabletop zijn de deelnemers bewust van hun rol tijdens een crisis, met wie zij moeten communiceren en wie besluiten neemt.

- **Een gerichte / kleinschalige praktijkoefening,** waarin een specifiek onderdeel van de cybersecurity- of incidentresponseprocessen wordt getest. Denk aan het terugzetten van backups door een technisch team of het melden van phishing mails door medewerkers.

- **Een organisatieoverstijgende oefening,** waarbij meerdere organisaties gezamenlijk optrekken in een gesimuleerd (groot) cyberincident. Dergelijke oefeningen kunnen meerdere dagen duren en zijn bijvoorbeeld gericht op het oefenen met de afstemming tussen ketenpartners tijdens een (inter-)nationale cybercrisis. Voorbeelden van dit soort organisatieoverstijgende oefeningen zijn de Overheidsbrede Cyberoefening, ISIDOOR en Cyber Europe.

Oefenen en testen

In de praktijk worden de termen ‘oefenen’ en ‘testen’ soms als synoniemen door elkaar gebruikt. Er is overlap, maar er zit een verschil in focus. Oefenen draait om het (nagenoeg altijd bewust) in praktijk brengen van (beveiligings-)maatregelen om de ervaring hiermee te vergroten, waar testen draait om het beoordelen van de effectiviteit, efficiency en kwaliteit van getroffen beveiligingsmaatregelen. Zie oefenen als het maken van een proefexamen, waar testen het examen is.

In bredere zin onderscheiden we, naast oefenen en testen, nog vier stappen om de vaardigheden van medewerkers en de organisatie aan te leren of te verbeteren: opleiden, trainen, oefenen, testen, evalueren en leren (OTOTEL).

Tijdens opleiding en training wordt medewerkers nieuwe vaardigheden aangeleerd. Oefenen en testen richten zich op het vergroten van de ervaring met, en toetsen van, deze nieuwe vaardigheden. Evalueren en leren staan in het teken van het identificeren en adopteren van verbeterpunten (die tijdens een oefening/test naar voren zijn gekomen). In deze publicatie leggen we de nadruk op ‘oefenen’, maar zie oefenen dus altijd in breder perspectief.

1. Schets een oefenplan

Als je net begint met oefenen, moet jouw organisatie hier wellicht nog aan wennen. Misschien heb je maar een beperkt budget om hiermee te starten en moet je nog bewijzen dat oefenen nuttig is. Dat is op zich geen probleem: ook met beperkte middelen kun je effectief oefenen. Daarbij is het wel belangrijk dat je jouw oefeningen prioriteert en afstemt op de behoeftes, doelstellingen en capaciteiten van jouw organisatie.

Om te beginnen met oefenen moet je eerst zicht hebben op het doel en de scope van jouw (eerste) oefening. Gebruik de onderstaande vragen om hier een beeld bij te vormen. Het helpt om deze vragen samen met jouw belangrijkste stakeholders, bijvoorbeeld de eigenaren van beheersprocessen, door te nemen en vervolgens samen te vatten in een (hoog-over) oefenplan.

Waar wil ik (als eerste) mee oefenen?

Oefenen is het meest doeltreffend als de oefening zich richt op zaken waar jouw organisatie nog beperkt ervaring mee heeft. Wat is voor jouw organisatie het meest doeltreffend? Denk hierbij aan:

- De (belangrijkste) risico's van jouw organisatie en de maatregelen die deze mitigeren.
- Een overzicht van incidenten en de tijdens-het-incident uitgevoerde activiteiten. Als je een activiteit al vaak uitvoert in praktijk, dan hoef je deze niet uitgebreid te oefenen.
- Een overzicht van eerder uitgevoerde oefeningen en de daaruitvolgende oefenresultaten en verbeterpunten.
- Recente veranderingen in de processen die relevant zijn voor jouw digitale weerbaarheid en die je met een oefening in praktijk wil brengen.

Wat wil ik bereiken door te oefenen?

Er zijn verschillende redenen om te oefenen. Denk vooraf na over de leerdoelen die je wilt realiseren, zoals:

- **Het vergroten van de ervaring van medewerkers**. Het hebben van beleid en procedures is één ding, maar weten hoe je ze effectief uitvoert tijdens een incident is iets anders. Alleen door te oefenen zorg je ervoor dat de betrokken medewerkers effectief kunnen handelen. Zeker met oog op het (natuurlijk) verloop van medewerkers is het goed om regelmatig te oefenen en zo de scherpte in het handelen te houden.

- **Rolbewustzijn**. De medewerkers van jouw organisatie onderschatten mogelijk cyberdreigingen of gaan ervan uit dat beveiliging vooral een taak is van IT-afdelingen, of in ieder geval niet van henzelf. Door te oefenen wordt voor de medewerkers duidelijk welke rol zij hebben tijdens een beveiligingsincident en waarom.

- **Verbeteren samenwerking tussen teams en ketenpartners.** Digitale weerbaarheid is nagenoeg altijd een teaminspanning en in het huidige, verweven digitale landschap vaak ook organisatie-overstijgend. Samen oefenen geeft de kans om te werken aan een effectieve samenwerking.

- **Verbeterpunten en aanscherping maatregelen.** Door te oefenen kun je zwakke plekken in de digitale weerbaarheid ontdekken. Misschien blijkt dat bepaalde processen en protocollen niet goed worden opgevolgd,zoals je incidentresponseplan, of dat de communicatie tussen afdelingen en ook externe partijen tijdens een crisissituatie hapert. Door daar zicht op te krijgen kun je gerichte verbeteringen doorvoeren.

- **Bewust bestuur.** Een crisisoefening biedt een uitgelezen kans om het bestuur te betrekken bij digitale weerbaarheid. Tijdens een crisisoefening heeft het bestuur een belangrijke, beslisvormende rol en wordt ze actief geconfronteerd met de risico's die voortkomen uit een cyberaanval. Hiermee wordt het bestuur bewust van haar rol en de noodzaak voor passende digitale weerbaarheid.

- **Compliance**. Oefenen is essentieel om te voldoen aan wet- en regelgeving of voor het certificeren voor beveiligingsstandaarden. De AVG, Cbw en ISO 27001 stellen bijvoorbeeld eisen aan het voorbereiden op incidenten en het testen van beveiligingsmaatregelen. Door regelmatig te oefenen en de bevindingen te documenteren, toon je de effectiviteit van jouw incidentresponsprocedures aan.

Wie moet er betrokken zijn?

De leerdoelen behaal je alleen als je de relevante stakeholders hebt betrokken. Maak een overzicht van alle relevante stakeholders en betrek ze bij het vormgeven en uitvoeren van de oefening.

Is mijn organisatie 'klaar' om te oefenen?

Oefenen is het meest effectief als de deelnemers al zijn getraind voor hun rol. Mochten de medewerkers nog niet voldoende op de hoogte zijn van hun rol en wat er van hen verwacht wordt, zet dan eerst in op training en opleiding.

Welke capaciteit heb ik (nodig)?

Een simpele tabletop-oefening gericht op basiscrisiscommunicatie vereist minder capaciteiten van jouw organisatie dan een meerdaagse, organisatie-overstijgende praktijksimulatie. Weet wat je van je organisatie kunt vragen om een passende oefenvorm uit te tekenen. Denk niet alleen aan geld en middelen, maar ook welke tijdsinspanning je van de deelnemers en faciliterende medewerkers vraagt.

Welke risico's accepteer ik?

Elke activiteit ,ook oefeningen, kunnen risico's inhouden. Verschillende vormen van oefenen brengen andere risico's met zich mee. Een oefening op basis van een tabletop brengt geen significante risico's voor de bedrijfsvoering. Het 'live' overschakelen op

noodstroom kan er echter voor zorgen dat de bedrijfsvoering stil komt te liggen indien dit niet vlekkeloos gaat. Breng deze risico's samen met de relevante stakeholders goed in kaart en beschrijf hoe je deze kunt mitigeren. Laat risico-eigenaren de oefening goedkeuren.

2. Ontwikkel de oefening en voer deze uit

Als je de contouren van de oefeningen hebt geschetst, dan kan je de oefening ontwikkelen en vervolgens in praktijk brengen. Maak hierbij gebruik van de volgende *good practices*.

Laat je inspireren

Elke oefening heeft zijn eigen invulling nodig, maar zal nooit volledig uniek zijn. We raden je aan om niet het wiel opnieuw uit te vinden. Maak gebruik van bestaande oefenvormen, frameworks en scenario's. Begin je net met oefenen? Maak dan gebruik van (eenvoudige) tabletop-oefeningen om groepsoefeningen vorm te geven gericht op proces en communicatie, en een kleinschalige oefening om te oefenen met de meer technische elementen.

Leer van sectorgenoten en ketenpartners

In jouw sector (of keten) wordt mogelijk al op bredere schaal geoefend. Voorbeelden van dit soort organisatieoverstijgende oefeningen zijn de Overheidsbrede Cyberoefening, ISIDOOR en Cyber Europe. Overweeg of je bij een dergelijke oefening aansluit om inspiratie op te doen. Mogelijk hoef je niet direct deel te nemen aan de oefening, maar kun je eerst een keer meekijken (als *observer*) en zo laagdrempelig aanhaken.

Maak het scenario realistisch, inclusief eventuele tijdsdruk

Geloofwaardigheid en relevantie helpt de deelnemer. Laat iedereen zijn echte rol spelen vanuit zijn expertise. Onder passende druk zul je bijvoorbeeld merken dat medewerkers niet uit de voeten kunnen met het reguliere proces en hiervan afwijken. Herkennen de deelnemers zich niet volledig in het scenario? Toon begrip voor de situatie, maar vraag hun alsnog mee te gaan in het scenario. Neem hun bevinding wel mee bij de evaluatie.

Begin klein, maar begin wel

Jouw oefenbehoefte is misschien breed en gevarieerd. Zeker als jouw organisatie nog niet veel ervaring heeft met oefenen, doe je er goed aan om op beperkte scope te oefenen. Wil je bijvoorbeeld beginnen met het oefenen van crisismanagement? Start dan niet met een organisatie-overstijgende praktijksimulatie, maar doorloop een fictief, overzichtelijk scenario in een tabletop. Door klein te beginnen bouw je oefenervaring op en kun je door een beperkte capaciteit te vragen van jouw organisatie laten zien wat de toegevoegde waarde van een oefening is.

Maak duidelijk dat het een oefening is

Waar een *test* een onverwacht karakter kan hebben, is het voor een *oefening* over het algemeen beter deze vooraf aan te kondigen. Maak duidelijk dat je tijdens het oefenen fouten mag maken (daar kan je van leren!) en dat hier dan ook geen negatieve consequenties aanzitten. Dit draagt bij aan de veilige leeromgeving die nodig is voor een succesvolle oefening. Maak ook op alle documenten die je gebruikt tijdens het oefenen, zoals een scenarioschets of een flipchart, duidelijk dat het een oefening betreft om te voorkomen dat deze uit hun context gebruikt worden.

Rolverdeling voor de oefening

De deelnemers van de oefening moeten hun volledige aandacht kunnen geven aan de oefening. Willen de deelnemers iets zeggen dat geen onderdeel is van de oefening, laat hen dit dan expliciet kenbaar maken. Zorg dat ondersteunende rollen,waaronder de oefenleider en observator, zelf geen deelnemer zijn van de oefening. Hecht waarde aan een goede ondersteuning: zonder sturing verliest een oefening snel zijn toegevoegde waarde.

Notuleer keuzes, knel- en verbeterpunten

Laat een observator vastleggen hoe de oefening verloopt. Schrijf bijvoorbeeld mee welke sleutelbesluiten er worden genomen, maar ook welke onduidelijkheden er waren tijdens het oefenen. Deze observaties zijn belangrijk voor een goede evaluatie en opvolging. Hou hierbij ook de leerdoelen in de gaten.

Win expertise in

Het ontwerpen en begeleiden van een succesvolle oefening vergt expertise en capaciteit. Heb je deze elementen niet (direct) beschikbaar in jouw organisatie? Overweeg dan of het voor jouw organisatie handiger is om de expertise zelf op te bouwen en/of een commerciële partij te betrekken:

- Je bouwt de expertise in jouw eigen organisatie bijvoorbeeld op door een betrokken medewerker een cursus of workshop te laten volgen om ervaring op te doen met het (organiseren en uitvoeren van) een oefening. Of draai mee met oefeningen bij sectorgenoten om kennis en ervaring uit te wisselen.

- Er zijn (commerciële) aanbieders die zich specialiseren in het geven van trainingen en het houden van oefeningen. Ook als je zelf voldoende expertise hebt, maar kampt met een gebrek aan capaciteit om een (grote) oefening voor te bereiden, dan kan een externe aanbieder een uitkomst zijn. Zorg er uiteraard voor dat die aanbieder jou kan leveren wat je zoekt, op basis van jouw hoog-over oefenplan.

3. Opvolging van de oefening

Neem de tijd om na de oefening stil te staan bij wat er goed ging en wat er in het vervolg beter kan. Op deze manier rond je de oefening op een prettige manier af en krijgen de deelnemers (en jij als organisator) de nodige input om te leren. Denk aan de volgende acties.

Evalueer de oefening

Geen enkele oefening is perfect. Geef de deelnemers de ruimte om te reflecteren op de oefening zelf. Wat was er goed geregeld aan de oefening, en wat kon er beter? Hebben de deelnemers bereikt wat zij wilden? En heeft het geleid tot het beoogde leerdoel? Houd ruimte aan het einde van de oefening om direct erna feedback te verzamelen in een groepssetting. Geef daarnaast de ruimte om aanvullende reflecties te geven in de dagen erna.

Maak een verbeterplan met concrete acties

Op basis van de bevindingen en ervaringen krijg je zicht op onvolkomenheden in jouw (beheers-)processen en maatregelen. Welke processen hebben extra aandacht nodig? Is er bijvoorbeeld onvoldoende communicatie tussen verschillende teams tijdens incidentrespons? Zijn er bepaalde technische maatregelen die onvolkomen zijn ingericht? Of zijn er juist hiaten in de training en opleiding die medewerkers hebben gevolgd?

Bespreek deze bevindingen met de aanwezigen tijdens de afsluiting van de oefening. Bespreek de bevindingen ook na de oefening met de relevante stakeholders en formuleer samen een verbeterplan. Prioriteer de verbeteracties en zorg er voor dat belangrijke (en afdeling-overstijgende) verbeteracties in managementrapportages terechtkomen, zodat bestuur en directie betrokken blijven.

Maak van oefenen een cyclisch proces

Oefenen is een activiteit die een bewezen bijdrage levert aan de digitale weerbaarheid van jouw organisatie. Zie oefenen dus ook niet als een eenmalige activiteit, maar als een cyclisch proces waarin je stapsgewijs werkt aan het versterken van je cyberweerbaarheid. Gebruik de handvatten uit paragraaf ‘schets een oefenplan’ om dit zo effectief mogelijk te blijven doen, waar je na verloop van tijd meer en meer kunt bouwen op jouw eerdere oefenervaring. Overweeg daarnaast een oefenkalender te maken, waarop je een aantal elementen vast inroostert, zoals een jaarlijkse crisisoefening.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Juni 2025