**Normenkader**
**Informatiebeveiliging en Privacy**
voor het onderwijs

# Keuzekaart securitytesten

| | Type test | Omschrijving | Doel en aanpak | Aanbevolen minimale volwassenheid normenkader IBP | Indicatie verloop testfase | Aanbevolen ervaring en capaciteit | Hulpmiddelen |
|---|---|---|---|---|---|---|---|
| Basis | Kwetsbaarhedenscan | Geautomatiseerde scans op technische kwetsbaarheden | In de breedte van de techniek opsporen van bekende technische kwetsbaarheden | Niveau 1 | 1-2 dagen | • Geen ervaring vereist<br>• Capaciteit nodig om uitkomsten op te volgen | NCSC, CIP |
| | Cybercrisis tabletop oefening | Korte oefening waarbij een kleine groep mensen een scenario doorloopt waarbij mondeling de ontwikkelingen van het incident of crisis worden beschreven | Processen en samenwerking tijdens een groot incident of cybercrisis testen en verbeteren | Niveau 1 | 2 uur | • Geen ervaring vereist<br>• Enige incident- en crisismanagementprocessen op papier | Kennisnet |
| | Penetratietest | Cyberaanval 'boven de radar' uitgevoerd met tools en handmatige acties | Gericht op één of beperkt aantal systemen. Uitputtend kwetsbaarheden opsporen en deze gebruiken om binnen te komen | Niveau 1 | 1-2 weken | • *Vulnerability scanning* uitgevoerd en bevindingen (grotendeels) opgevolgd | NCSC UK |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Geavanceerd | Purple teaming | Cyberaanval uitgevoerd door een 'red team' (ingehuurde ethische hackers) in samenwerking met het 'blue team' (het eigen CERT of SOC) | Identificeren van aanvalspaden en het verbeteren van de detectie- en response-effectiviteit van het 'blue team' om daarmee de cyberweerbaarheid te verhogen | Niveau 2 | 1-10 weken | • *Vulnerability scanning* en eventuele pentests uitgevoerd en bevindingen (grotendeels) opgevolgd<br>• Monitoring en detectie-capaciteit ingericht en operationeel | DNB |
| | Simulatie cybercrisisoefening | Oefening waarbij de gehele escalatie van een crisis wordt getest en men daadwerkelijke acties kan uitvoeren | Testen en verbeteren samenwerking op alle niveaus binnen en tussen organisaties om voor te bereiden op een cybercrisis | Niveau 2 | 1-3 dagen | • Tabletopoefening gedaan en verbeterpunten (grotendeels) opgevolgd<br>• Crisismanagement proces op papier | Op dit moment is er nog geen hulpmiddel voor het funderend onderwijs beschikbaar. Voorbeelden uit andere sectoren: OZON en ISIDOOR. |
| | Red teaming | Cyberaanval 'onder de radar' gebaseerd op generieke dreigingsinformatie | Realistisch simuleren van een specifieke actor om te kijken in hoeverre de kroonjuwelen hiertegen beschermd zijn en de organisatie als geheel hiervan te laten leren | Niveau 2 | 7-14 weken | • *Vulnerability scanning* en pentests uitgevoerd en bevindingen (grotendeels) opgevolgd<br>• Monitoring en detectie-capaciteit ingericht en operationeel<br>• Genoeg capaciteit om een 'white team' te kunnen leveren die los staan van het blue team | BZK |

*Deze keuzekaart is gebaseerd op de Keuzekaart cybersecurity weerbaarheidstesten van SURF.*