Keuzekaart security testen

Vragen?
Mail sec@surf.nl

	Type test	Kenmerk	Doel / aanpak	Scope	NIST-functies	Minimale volwassenheid SURFaudit toetsingskader	Indicatie verloop test	Aanbevolen ervaring en capaciteit	Hulpmiddelen
Basisniveau	**Vulnerability scanning**	Geautomatiseerde scans op technische kwetsbaarheden	In de breedte van de techniek opsporen van bekende technische kwetsbaarheden	Techniek	Identify, protect	Niveau 1 of hoger	1-2 dagen	• Geen ervaring vereist • Capaciteit nodig om uitkomsten op te volgen	Handreiking kwetsbaarheidsscan
	Deelname Coordinated Vulnerability Disclosure (CVD)	Kaders en informatie publiceren om vrijwilligers te laten zoeken naar kwetsbaarheden	Gelijk aan vulnerability scanning, maar een focus op het open staan voor meldingen van vrijwilligers	Techniek	Identify, protect	Niveau 1 of hoger	Voortdurend	• Gelijk aan vulnerability scanning	HALON, handreiking CVD
	Cybercrisis of -incident 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	Mensen, processen	Respond	Niveau 1 of hoger	2 uur (uitvoering)	• Geen ervaring vereist • Enige incident- en crisismanagementprocessen op papier	NOZON, Tabletop oefeningen handleiding
	Penetration testing (pentest)	Cyberaanval “boven de radar” uitgevoerd met tools en handmatige acties	Gericht op 1 of beperkt aantal systemen. Uitputtend kwetsbaarheden opsporen en deze gebruiken om binnen te komen	Techniek	Identify, protect, detect	Niveau 1 of hoger	1-2 weken	• Vulnerability scanninguitgevoerd en bevindingen (grotendeels) opgevolgd	Whitepaper pentesten
Geavanceerde testen	**Purple teaming (PT)**	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 cyber weerbaarheid te verhogen	Techniek, mensen, processen	Identify, protect, detect, respond	Niveau 2 of hoger	1-10 eken	• Vulnerability scanning en evt. pentests uitgevoerd en bevindingen (grotendeels) opgevolgd • Monitoring en detectie- capaciteit ingericht en operationeel	Purple teaming guide (TIBER)
	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	Techniek, mensen, processen	Identify, protect, respond, recover	Niveau 2 of hoger	1 tot 3 dagen (uitvoering)	• Tabletop oefening gedaan en verbeterpunten (grotendeels) opgevolgd • Crisismanagement proces op papier	OZON, Whitepaper Cyber Crisis Exercises
	Red teaming (RT) / Advanced red teaming (ART)	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	Techniek, mensen, processen	Identify, protect, detect, respond	Niveau 2 of hoger	7–14 weken	• VS en pentest uitgevoerd en bevindingen (grotendeels) opgevolgd • Monitoring en detectie- capaciteit ingericht en operationeel • Genoeg capaciteit om een white team te kunnen leveren die los staan van het blue team	RT-raamwerk ART (nog in ontwikkeling)

Deze keuzekaart is gebaseerd op de Keuzekaart Securitytesten uit de Toolkit van Ministerie BZK