Auteur: Rob Wassink is sinds 2019 werkzaam bij De Nederlandsche Bank als TIBER-NL Test Manager. Daarnaast geeft hij parttime les bij InHolland. Hij werkte eerder bij NN Group als Information Security Officer. Hij is bereikbaar onder j.b.wassink@dnb.nl.

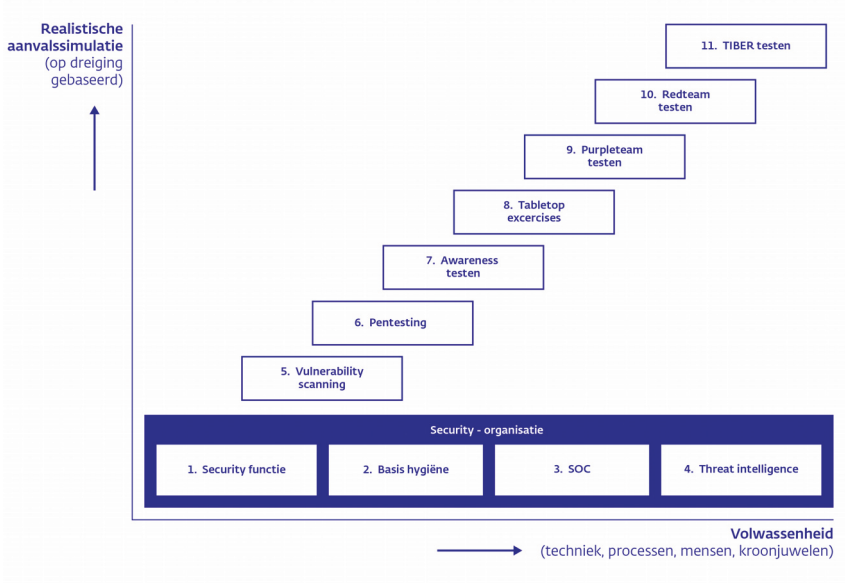
Ben ik voorbereid op een cyberaanval?

Het doel van securitytesten is de kwetsbaarheid van organisaties te onderzoeken. Met het uitvoeren van securitytesten en het oplossen van bevindingen wordt tevens de cyberweerbaarheid van organisaties verhoogd. In de Good Practise Informatiebeveiliging van DNB komt het belang van securitytesten ook duidelijk aan de orde. Er zijn verschillende type securitytesten om kwetsbaarheden van technische (IT) systemen, medewerkers en (business)processen binnen de organisatie te onderzoeken.

Dit artikel beschrijft aan de hand van het model in figuur 1 kort welke soorten security-testen er zijn en hoe ze onderling samenhangen. Het op ervaring gebaseerde model kan worden gebruikt om tot een securitytest-roadmap te komen die organisaties helpt zich stap voor stap beter voor te bereiden op een cyberaanval.

Een model om tot een securitytest-roadmap te komen

Op de horizontale as van figuur 1 wordt de mate van volwassenheid van de security-organisatie weergegeven. De verticale as toont het 'trappetje' van steeds realistischer wordende securitytesten (aanvalssimulaties). De volgorde van stappen is niet in beton gegoten. Het kan goed zijn dat bepaalde testen regelmatig terugkomen, terwijl de meest geavanceerde testen niet jaarlijks worden uitgevoerd. Het gaat erom dat de organisatie optimaal leert van de testervaring en zich continu blijft verbeteren.



Figuur 1: Model om tot een securitytest-roadmap te komen (Bron: DNB TIBER-team).

Eerst de security-organisatie op orde brengen

Een volwassen security-organisatie heeft vier basisvoorwaarden ingevuld (figuur 1: blokje 1 t/m 4):

1. **De security-functie**, meestal een CISO krijgt de opdracht om een volwassen information security-organisatie te beschrijven. Het bestuur is verantwoordelijk voor een goede implementatie.

Het doel is beheerste bedrijfsvoering doordat de cyberweerbaarheid van de organisatie in lijn is met de cyberdreiging.

2. Een volwassen security-organisatie heeft een goede **basishygiëne** en voldoet daarmee aan de vereiste ISO27001- en ISO27002-normering, of een afgeleide daarvan zoals de NEN7510 of de BIO.
   Bij DNB zien we de cyberdreiging ten aanzien van de sector verder toenemen terwijl de basismaatregelen bij verschillende financiële instellingen niet altijd op orde zijn of in lijn met bestaande cyberdreiging (1).
   Het is belangrijk voor organisaties om een goed beeld te hebben van de kritieke functies (kroonjuwelen) en onderliggende systemen en services. Deze vormen het doelwit voor verschillende internationale hackersgroepen.
3. **Een Security Operating Center (SOC)** of soortgelijk team doet aan logging en monitoring van events, en verzorgt de operationele incident response na detectie van een security incident. De SOC-functie kan intern aanwezig zijn of (deels) uitbesteed zijn bij een security provider.
4. **Threat intelligence** kan de organisatie van relevante dreigingsinformatie voorzien zodat tijdig geanticipeerd kan worden op nieuwe en veranderende dreiging. Gebaseerd op deze informatie kunnen de juiste maatregelen getroffen worden en kan wanneer deze samen worden genomen, de cyberweerbaarheid van de organisatie worden ingeschat. Meestal wordt hierbij een onderverdeling gemaakt naar strategisch, tactisch en operationeel niveau. Ook wordt er gekeken op verschillende onderdelen van de organisatie: techniek, fysiek, processen en mensen.

Met securitytesten verhoog je de cyberweerbaarheid

In de Good Practise Informatiebeveiliging van DNB komt het belang van securitytesten aan de orde. Als de vier basisvoorwaarden voor de security-organisatie zijn ingevuld en de volwassenheid aantoonbaar toeneemt, kunnen technische securitytesten overgaan in steeds realistischer wordende aanvalssimulaties (Fig. 1: blokje 5 t/m 11):

5. Met **vulnerability scanning**, een technische securitytest, kunnen bekende kwetsbaarheden met scanning tools geautomatiseerd worden opgespoord in configuraties binnen het IT- en applicatielandschap van de organisatie.
6. Bij **penetratietesten (pentesten)** wordt niet alleen gezocht naar kwetsbaarheden, maar ook of deze gebruikt kunnen worden om in te breken. Vaak gebeurt dat met een beperkte scope op bijvoorbeeld een IT-systeem of applicatie.
7. In security **awareness-testen** worden ook eindgebruikers en het management in de scope meegenomen. Deze testen worden gebruikt om het security-bewustzijn van de mensen te verhogen met als doel een gedragsverandering te realiseren. Dit kan bijvoorbeeld via trainingen tijdens 'onboarding', via online campagnes, of door middel van social engineering en (spear) phishing testen.
8. Tijdens **tabletop exercise**s gaat het crisismanagementteam (CMT) om tafel zitten en wordt een scenario geoefend waarbij een security-incident een crisis heeft veroorzaakt. Een geactualiseerd CMT en bijbehorend crisismanagementplan zijn een vereiste voor elke organisatie. Het regelmatig oefenen van verschillende scenario's, waaronder cyberaanvallen die de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) ondermijnen, verhoogt de weerbaarheid van organisaties.
9. Voor **purpleteam-testen** huurt de organisatie 'ethical hackers' in (een 'redteam') om met het SOC en de verdedigende organisatie (het 'blueteam') te testen of maatregelen in de praktijk ook echt effectief zijn (Red + Blue = Purple, vandaar deze naam). Denk aan detectiemaatregelen en of deze zijn afgestemd op de laatst bekende aanvalstechnieken die volgen uit threat intelligence.
10. Bij **redteam-testen** huurt de organisatie wederom ethical hackers in die minimaal één aanvalsscenario spelen, maar nu zonder het blueteam vooraf op de hoogte te stellen. Derhalve nog realistischer. Redteam-testen worden bijna altijd afgesloten met purpleteaming om het blueteam inzicht te geven in wat er is gedaan en ze de kans te geven om met terugwerkende kracht van de test te leren.
11. **TIBER-testen** (2) zijn van toepassing op bedrijven die van vitaal belang zijn voor een stabiele samenleving. Hierbij worden een aantal elementen toegevoegd aan het reguliere redteamen. Er wordt getest op de live productie systemen, er is begeleiding vanuit de competente autoriteit (zoals DNB). Slechts een klein team binnen de organisatie weet van de test, waaronder iemand uit het bestuur. Het verbeterplan krijgt hiermee automatisch aandacht op bestuurdersniveau. De test is gebaseerd op threat intelligence zodat alleen realistische aanvallen worden nagespeeld. De uitkomsten van de test worden na afloop gedeeld met de toezichthouder.

Een securitytest-roadmap om de organisatie voor te bereiden

Onder aansturing van de CISO kan een securitytest-roadmap gemaakt worden. Deze roadmap geeft een meerjarig inzicht in welke securitytesten uitgevoerd kunnen worden. Door het volgen van de roadmap, zal de organisatie stap voor stap volwassener worden. En door toenemende weerbaarheid steeds beter voorbereid zijn op een echte cyberaanval.

Referenties

(1) https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/
(2) https://www.dnb.nl/voor-de-sector/betalingsverkeer/tiber-nl/