PLATFORM VOOR SECURITYPROFESSIONALS

SECURITY MANAGEMENT



Cyberaanval! En dan? Wat je ervan kunt leren

Updates en patches zijn cruciaal

Hoe veilig is ChatGPT eigenlijk?

UITGELICHT CYBERSECURITY

Jaargang 46 | #3 | juni 2023

Benaderingen van vakgebied in model vastgelegd

Driepoortenmodel onder de loep

Voor doorgewinterde beveiligingsprofessionals is het soms al lastig om de terminologie die binnen het vakgebied securitymanagement gebruikt wordt te begrijpen, laat staan voor de beginnende professional. Wat de materie nog complexer maakt zijn de verschillende benaderingen die gehanteerd worden. Tijd dus om wat licht in de duisternis te laten schijnen.

Door Nick F. Barelds en Berndt Rif

In dit artikel worden de belangrijkste termen uit het vakgebied securitymanagement geduid door middel van het zogeheten driepoortenmodel waarin de verschillende benaderingen van het vak een plek krijgen. Het is wel goed om in ogenschouw te nemen dat een model altijd een gesimplificeerde weergave van de werkelijkheid is en nooit alle facetten kan belichten. In beginsel is het model bruikbaar vanuit het perspectief van integrale beveiliging. Het lastige is wel dat, afhankelijk van de expertise van de beveiligingsprofessional, er soms verschillende definities gehanteerd worden voor hetzelfde onderwerp.

Dreigingsscenario's

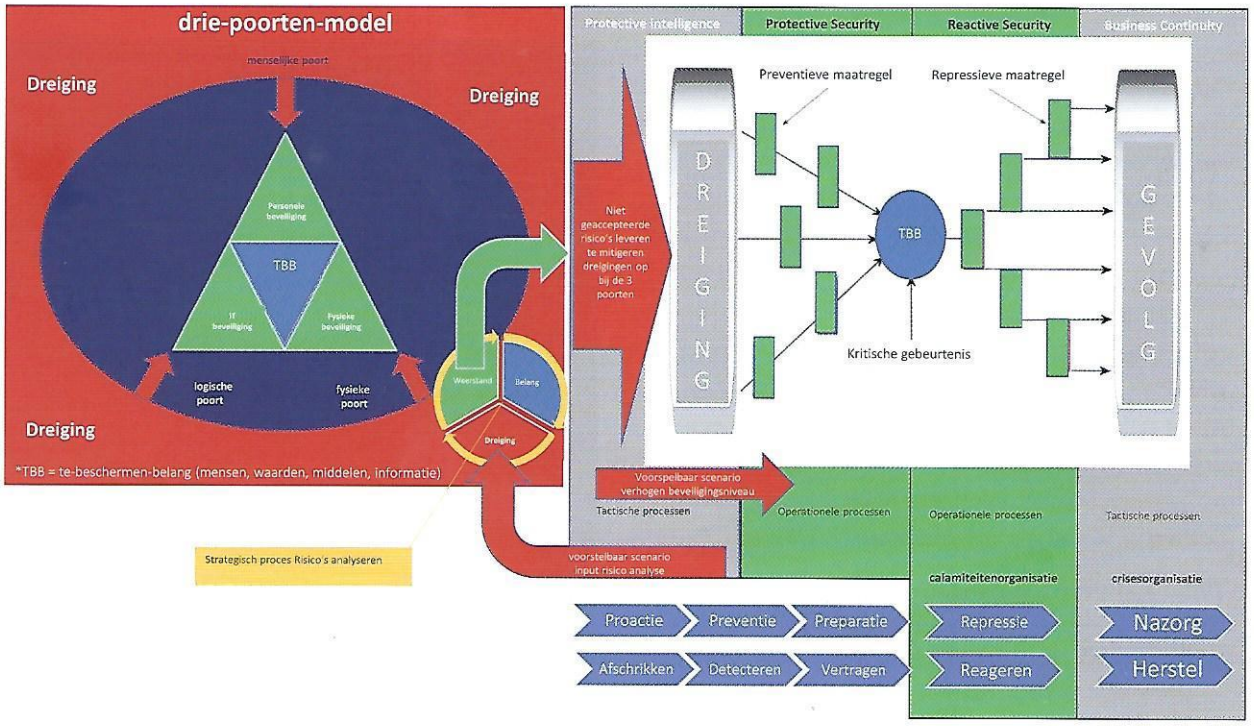
Het driepoortenmodel is, als het gaat om integrale beveiliging, tussen 2008 en 2012 door De Nederlandsche Bank geïntroduceerd tijdens bijeenkomsten van de Vereniging Beveiligingsprofessionals Nederland (VBN) en de ASIS Benelux Chapter. Het idee is dat kwaadwillenden zich toegang tot een organisatie kunnen verschaffen door middel van drie poorten: de fysieke poort, de logische poort en de menselijke poort. Inmiddels komen wij ook andere woorden tegen – verbasteringen – die de poorten beschrijven waardoor er weer onduidelijkheid ontstaat. Belangrijk bij dit model is dat er gekeken wordt naar dreigingen. Er is nog geen sprake van een risico-afweging.

Om dreigingen goed in kaart te kunnen brengen, is het noodzakelijk dat een beveiligingsprofessional in staat is om, als input voor het analyseren van de risico's, zelfstandig voorstelbare dreigingsscenario's op te stellen. Dit betekent dat van de actoren die de organisatiebelangen kunnen aantasten, de motivatie en de capaciteit in kaart worden gebracht.

Heeft een actor zowel de motivatie als de capaciteit om de organisatiebelangen aan te tasten, dan is er sprake van een dreiging (1 of 0). Bij het in kaart brengen van dreigingen gaat het om het verzamelen van informatie die de beveiligingsprofessional, en dus ook de organisatie, had kunnen en moeten kennen. Dit betekent dat het om informatie gaat waar de beveiligingsprofessional toegang toe heeft in open bronnen of kan krijgen op basis van collegiale uitwisseling tijdens bijeenkomsten van vakverenigingen. Voorstelbare dreigingsscenario's vormen 99,99 procent van de input voor het analyseren van risico's.

Laagste niveau

Het stelsel bewaken en beveiligen, zoals dat in regelgeving is beschreven, heeft als uitgangspunt dat de verantwoordelijkheid voor integrale beveiliging op het laagste niveau ligt. Dat wil zeggen: bij de medewerker en bij de eigen organisatie. Pas als er dreigingen geïdentificeerd zijn op basis van



Security Management Model (2022, Barelds & Rif

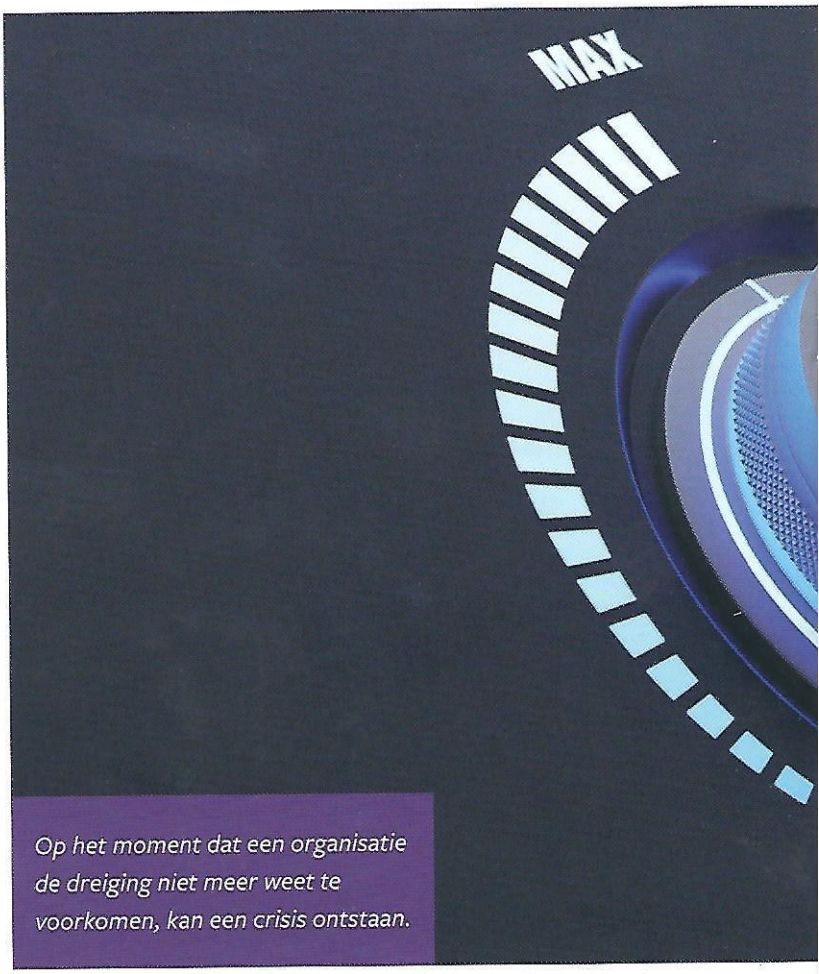
voorstelbare scenario's die niet op het laagste niveau gemitigeerd kunnen worden, komen overheidsdiensten in beeld. Deze overheidsdiensten dienen dan wel eerst proactief door de beveiligingsprofessional geïnformeerd te worden over restrisico's, op basis van voorstelbare dreigingsscenario's die niet door de eigen organisatie gemitigeerd kunnen worden.

Daarbij komt ook de term voorspelbare dreigingsscenario's naar voren. Bij deze categorie gaat het om dreigingen waarvoor veiligheidsdiensten concrete informatie hebben: er is informatie dat er iets staat te gebeuren, alleen tijd en locatie zijn nog niet duidelijk. Dat wil zeggen dat er naast motivatie en capaciteit nu ook informatie is over door de tegenstander getroffen voorbereidingen. Om deze informatie hoeft de beveiligingsprofessional niet te vragen. Als veiligheidsdiensten concrete informatie hebben waaruit blijkt dat er mogelijk iets staat te gebeuren, dan voorziet het stelsel er ook in dat de overheid maatregelen moet treffen om de voorspelbare dreiging te mitigeren. Daar hoort ook bij dat de organisatie of het doelwit, als dat een persoon is, geïnformeerd worden. Op dit moment is de minister van Justitie en Veiligheid bezig, naar aanleiding van een onlangs door de Onderzoeksraad voor Veiligheid uitgebracht rapport, met een herziening van het stelsel bewaken en beveiligen.

Analyseren

Het lijnmanagement van een organisatie is verantwoordelijk om, op basis van voorstelbare scenario's, een risicoanalyse op te stellen. In de praktijk is het dan de beveiligingsprofessional die de risicoanalyse maakt. Uit de beschrijving van het stelsel bewaken en beveiligen blijkt dat voor het verzamelen van (dreigings)informatie op het vlak van voorstelbaarheid het niet nodig is om veiligheidsdiensten te bevragen. De voorstelbare dreigingsinformatie is beschikbaar in open bronnen. Wel belangrijk bij het opstellen van een risicoanalyse is dat, bij de weging van 'te beschermen belang – dreiging – weerstand', de restrisico's goed beschreven worden. Als het goed is, staan in het beveiligingsplan, dat geschreven is op basis van een eerdere risicoanalyse, alle te treffen en getroffen beveiligingsmaatregelen beschreven. Belangrijk is ook dat bij iedere beveiligingsmaatregel ook de restrisico's vermeld staan. Een voorbeeld is het verschil tussen een toegangsverleningsregime en een toegangscontroleregime. Bij toegangsverlening krijgen gebruikers van (elektronische) sleutels toegang tot een locatie, bij toegangscontrole wordt pas toegang gegeven als duidelijk is dat de gebruiker en het toegangsverleningsmiddel bij elkaar horen. Het restrisico van een toegangsverleningsregime is dat nooit duidelijk is wie er bij een locatie binnen zijn, alleen welke toegangsverleningsmiddelen er gebruikt zijn (als dit vastgelegd is). Hetzelfde gaat op voor een deur en een *circle lock*. Bij een deur die legitiem geopend wordt, is nooit vast te stellen hoeveel mensen er zijn meegelopen. Bij een *circle lock* is duidelijk dat er altijd maar een persoon toegang heeft gekregen (als er sprake is van meting dat er maar een persoon in de *circle lock* staat). Een risicoanalyse is niet compleet als de beschrijving van restrisico's ontbreekt.

Door de beveiliging van de eigen organisatie te baseren op de uitgangspunten van het stelsel bewaken en beveiligen, lijkt het werk van de beveiligingsprofessional er eenvoudiger op te worden. Hij of zij kan immers alleen beschikken over informatie uit open bronnen – voorstelbare scenario's – waardoor het bevragen van inlichtingen- en veiligheidsdiensten (AIVD, MIVD, politie, NCTV) niet zinvol is voor het krijgen van input voor de risicoanalyse en het beveiligingsplan. Er mag namelijk vaak geen informatie uit gesloten bronnen verstrekt worden. Dit maakt dat een organisatie de beveiligingsprofessional in staat moet stellen om uit open bronnen informatie te verzamelen. Daar hoort ook het bezoeken van bijeenkomsten die vakverenigingen organiseren bij.



Op het moment dat een organisatie de dreiging niet meer weet te voorkomen, kan een crisis ontstaan.

Redteaming

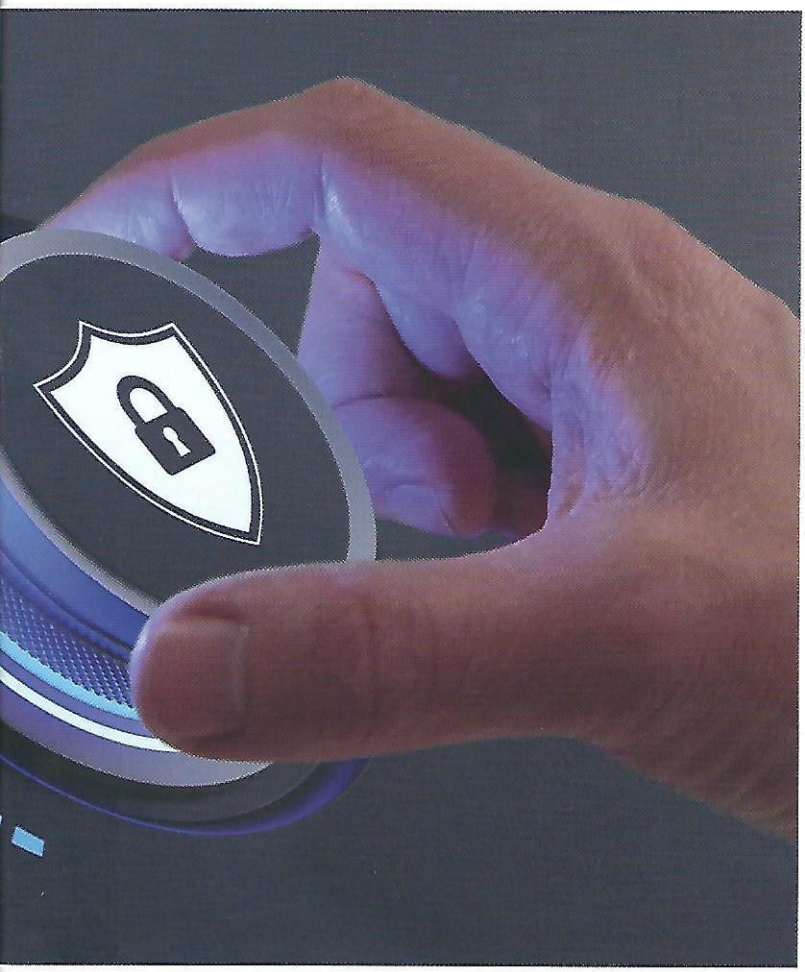
Verder kan de beveiligingsprofessional zelf 'nieuwe' realistisch voorstelbare dreigingen identificeren door middel van structurele *redteaming*. Dit maakt *redteaming* in deze context een operationeel (inlichtingen)middel om, op een open en transparant herleidbare manier, inlichtingen te verzamelen. Een organisatie die geen middelen vrijmaakt voor de inrichting van dit proces, maakt het voor de securityprofessional lastig om een goede risicoanalyse en een goed beveiligingsplan op te stellen. Bovendien kan de organisatie, als wij naar het stelsel bewaken en beveiligen kijken, niet goed aangeven welke risico's niet zelfstandig gemitigeerd kunnen worden.

Als wij ervan uitgaan dat alle voorstelbare dreigingen in kaart zijn gebracht, er een beveiligingsplan is waarin beschreven wordt welke dreigingen gemitigeerd worden en welke restrisico's er zijn, dan kan enerzijds risicoacceptatie plaatsvinden en kan anderzijds duidelijkheid gegeven worden aan externe (overheids)diensten over de vraag waar de te treffen benodigde maatregelen de lokale verantwoordelijkheid van de organisatie overstijgen.

Wat, als dit zuiver is uitgewerkt, niet mag ontbreken is een escalatieplan. Dit escalatieplan gaat over de eventueel additioneel te treffen maatregelen op het moment dat er informatie binnenkomt over een voorspelbare dreiging. Deze informatie kan van een veiligheidsdienst afkomstig zijn maar ook van een medewerker of vanuit het eigen professionele netwerk. Belangrijk is ook om te borgen, mocht het escalatieplan beschrijven dat er extra mensen of middelen noodzakelijk zijn, dat er vooraf met leveranciers afspraken zijn gemaakt over het leveren van diensten of producten. Bovendien is het van belang dat er afspraken zijn gemaakt met ketenpartners in het veiligheidsdomein.

Identificeren van dreigingen

Om dreigingen goed in kaart te kunnen brengen is het noodzakelijk dat een beveiligingsprofessional in staat is om, als input voor het analyseren van risico's, zelfstandig voorstelbare dreigingsscenario's op te stellen. Voor het verzamelen van deze scenario's is het niet nodig om veiligheidsdiensten te bevragen. De voorstelbare dreigingsinformatie is beschikbaar in open bronnen. Pas als er dreigingen geïdentificeerd zijn, op basis van voorstelbare scenario's, die niet op het laagste niveau gemitigeerd kunnen worden, komen overheidsdiensten in beeld. De beveiligingsprofessional kan de ketenpartners informeren over restrisico's, op basis van de voorstelbare dreigingsscenario's, die niet door de eigen organisatie gemitigeerd kunnen worden.



De Haagse Methodiek (DHM) noemt het document waar deze afspraken in beschreven staan het Plan Externe Beveiligingsorganisatie (EBO). Niets is zo lastig als op het moment dat het spannend gaat worden, het wiel te moeten uitvinden.

BowTie-methodiek

In het model staat, als het gaat om het treffen van preventieve en repressieve maatregelen, de bekende BowTie. In de BowTie worden, als het goed is, alle benodigde beveiligingsmaatregelen opgenomen die nodig zijn om een dreiging te mitigeren (op basis van motivatie en capaciteit van de tegenstander). Essentieel is om maatregelen waar geen budget of draagvlak binnen de organisatie voor is, wel te laten staan en de kleur rood te geven. Dit maakt dan meteen duidelijk waar risico-acceptatie dient plaats te vinden.

De door De Haagse Methodiek (DHM) gebruikte INCIDETAR-methode sluit ook mooi aan op de BowTie. Beide kunnen elkaar versterken. Belangrijk is wel om het verschil tussen incident, calamiteit en crisis goed in beeld te brengen. Bij een incident is er, na detectie, een snelle respons mogelijk waardoor het te beschermen belang niet wordt aangetast. Om het maar even tastbaar te maken, detectie maakt het als preventieve maatregel mogelijk om te voorkomen dat een dief de kluis kan bereiken. Er zijn instructies die afdoende zijn om in te grijpen.

Bij een calamiteit is, uitgaande van de BowTie, het te beschermen belang aangetast maar het gevolg is nog niet opgetreden. Er zijn nog repressieve maatregelen die kunnen voorkomen dat de dief met de buit het gebouw kan verlaten.

Op het moment dat de eigen organisatie niet meer in staat is het gevolg te voorkomen, wordt een calamiteit een crisis. Als dat niet meer te voorkomen is, heeft de beveiliging gefaald. Beveiliging heeft immers als doel dat het gevolg van onbevoegd menselijk handelen niet kan optreden. Realiseer je wel dat iedere sector, en soms zelfs organisaties binnen een sector, afwijkende definities kunnen hanteren van deze drie begrippen (incident, calamiteit, crisis). Vraag dus altijd, voordat je conclusies trekt, naar de definities die gehanteerd worden. Ook kan zo'n gevolg veroorzaakt worden door een domino- of cascade-effect dat buiten de organisatie ligt. In dat geval heeft de beveiliging niet gefaald, maar moet deze wel naar behoren reageren.

Doorontwikkeling vakgebied

Het model, waarin verschillende benaderingen zijn samengebracht, is slechts een versimpelde weergave van de werkelijkheid. Waar aan dit model een bedrijfskundig uitgangspunt ten grondslag ligt, en de vraag welke (deel) processen de securityprofessional tot zijn beschikking heeft, is DHM een manier om via de INCIDETAR-lijn maatregelen te plotten op operationeel niveau.

Het zou mooi zijn als de komende periode de relatie tussen de INCIDETAR-lijn vanuit DHM en de maatregelen vanuit de processen 'toegang verlenen', 'dreigingen herkennen', 'alarmen verifiëren' en 'incidenten afhandelen' transparant gemaakt kan worden. Daarbij is het ook goed om wat als (onwenselijk) gevolg binnen de BowTie-methodiek beschreven is in relatie tot de businesscontinuïteit, verder uit te werken. In dit model is businesscontinuïteit buiten beschouwing gelaten. De reden daarvoor is het uitgangspunt dat beveiliging als doel heeft incidenten te voorkomen en, als dat niet mogelijk blijkt, zo snel mogelijk te mitigeren. Als dat niet lukt, komt businesscontinuïteit als proces in beeld.

Nick Barelds BPM MIHR is docent aan de Haagse Hogeschool. Berndt Rif MSc MBA MSec CPP geeft gastcolleges aan de Haagse Hogeschool, de Hogeschool Inholland (tevens lid Beroepenveldcommissie), Saxion Hogeschool en de TU Delft.