



Crisis in de praktijk

Het gouden uur van een cybercrisis, en de zes stappen die het bepalen

CyberBusters B.V. · praktijkstuk · versie 1.0

Een crisis gaat in de eerste uren zelden mis op techniek, en ook niet op kalmte.

Hij gaat mis op bevoegdheid, en daarna op opvolging. Er zit een zaal vol mensen die weten wat er moet gebeuren, en niemand die zeker weet of hij het mag laten doen. Wat daarna wordt besloten, verdwijnt vaak in de zaal in plaats van bij iemand terecht te komen.

Dit stuk beschrijft die keten, en hoe je hem klokt.

Samenvatting

Over gedrag onder druk is goed nagedacht. Er bestaat een onderbouwd model van crisisvaardigheden, met onderzoek uit de brandweer, de luchtvaart en de rampengeneeskunde eronder. Dat model beschrijft hoe mensen zich houden als het spannend wordt, en het beschrijft dat goed.

Dit stuk gaat over iets anders, een laag eronder. Niet hoe het team zich gedraagt, maar wat er met het besluit gebeurt: wie het nam, wie het uitvoerde, en of iemand het nakeek. Dat is geen eigenschap van mensen maar van de keten ertussen, en in tegenstelling tot gedrag laat die keten zich kloppen.

Zes stappen vormen die keten: beeld, oordeel, besluit, opdracht, controle, overdracht. De eerste vijf komen uit de Nederlandse crisisbeheersing en staan bekend als BOBOC. De zesde staat in geen enkel model en komt in elke lange crisis voor.

1. Een woensdagmiddag in oktober

Op woensdag 21 oktober 2026 werden twee kritieke kwetsbaarheden in PHP openbaar, vóór de geplande publicatie en met werkende proof-of-conceptcode erbij. Het NCSC schreef die ochtend dat ze met een eenvoudig POST-verzoek te misbruiken zijn, en meldde om 11:03 nog geen actief misbruik te hebben gesignaleerd. Patches waren er op dat moment nog niet.

Wat er daarna gebeurde is beter gedocumenteerd dan de meeste crises, want twee organisaties schreven hun besluiten op met het tijdstip erbij.

Het NCSC haalde zijn eigen website uit voorzorg offline. De hostingpartij Mijndomein besloot om 13:35 dat alle klantwebsites preventief offline zouden gaan tot de update er was; om 14:30 stond dat er. De motivering schreven ze erbij: een tijdelijke onbereikbaarheid is voor ons een kleiner risico dan de mogelijkheid van een inbraak. In de loop van de avond rolden ze de nieuwe PHP-versies uit, en pas de volgende ochtend om 11:20 stond er dat het was opgelost.

Lees dat verloop nog eens met de zes stappen uit dit stuk ernaast. ****Beeld:**** draaien wij een kwetsbare versie, en waar. ****Oordeel:**** onbereikbaarheid tegen de kans op een inbraak. ****Besluit:**** om 13:35, door iemand die het mocht. ****Opdracht:**** om 14:30 stond het er. ****Controle:**** de update erop, de sites terug. ****Overdracht:**** het liep door de nacht en was pas de volgende ochtend klaar.

Dit is geen uitzonderlijke crisis. Hij staat hier omdat hij toevallig is opgeschreven, en omdat elke stap die verderop wordt beschreven er met een tijdstempel in terug te vinden is.

2. Waar de eerste uren verdwijnen

In de traumazorg heet het eerste uur het gouden uur. Of die zestig minuten precies kloppen is in de literatuur omstreden, en daar gaat het hier niet om. Het gaat om de reden dat het werkt: in dat uur gebeurt niets briljants. Er ligt een volgorde vast, iedereen kent zijn rol, en niemand hoeft te vragen of hij mag.

Een cybercrisis heeft ook zo'n uur, en daar ligt die volgorde meestal niet vast.

Vraag na afloop van een echte crisis waar de tijd is gebleven, en het antwoord gaat zelden over techniek. Het gaat over de periode waarin iedereen wist wat er zou moeten gebeuren en niemand het in gang zette.

Die periode heeft een oorzaak die zich makkelijk laat benoemen en moeilijk laat oplossen: het is onduidelijk wie wat mag. Op papier staat het er vaak wel. In de kamer zelf is het de vraag of dit het geval is waarop die regel ziet, of de situatie erg genoeg is, en of degene die het mag ook bereikbaar is.

Het gevolg is een besluit dat te laat valt, of dat valt zonder dat iemand het draagt. Dat tweede is het vervelendst, want dan gebeurt er niets terwijl iedereen denkt dat het geregeld is.

3. Gedrag is de helft, structuur de andere

Een team dat kalm blijft, overzicht houdt en kan improviseren, heeft een betere uitgangspositie. Dat spreekt vanzelf en het is goed onderzocht. Wij vervangen dat niet en claimen dat terrein niet.

Maar kalmte zonder bevoegdheid levert niets op. Een team kan in volmaakte rust vaststellen dat de productielijn eruit moet, en vervolgens veertig minuten wachten tot iemand terugbelt. Dan was het probleem niet het gedrag.

Daarom kijken wij naar de keten: van de eerste melding tot een maatregel die aantoonbaar is uitgevoerd. Niet omdat gedrag er niet toe doet, maar omdat de keten het deel is dat je kunt vastleggen en volgend jaar opnieuw kunt meten.

Dat is ook wat het gouden uur in de traumazorg doet. Niet de kalmte van de arts is daar vastgelegd, maar de volgorde eromheen. Structuur maakt gedrag minder bepalend, en dat is precies wat je wilt op een nacht waarin niemand op zijn best is.

4. De zes stappen

Zes stappen. Vijf ervan zijn BOBOC, de werkwijze uit de Nederlandse crisisbeheersing: beeldvorming, oordeelsvorming, besluitvorming, opdrachtverstrekking en controle. De laatste twee ontbreken in modellen die over gedrag gaan, en het zijn precies de stappen waar een besluit verdampt.

De zesde stap is de overdracht. Die staat in geen enkel model en komt in elke crisis voor die langer duurt dan een dienst.

	Stap	Wat er misgaat	Wat je meet
B	Beeld	Wat is er gebeurd? Vier groepsapps en een telefoonlijst zijn geen beeld. Zonder afgesproken momenten schuift het beeld per persoon, en dan onderhandelen twee mensen over een feit in plaats van over een besluit.	Hoe lang tot er één beeld is, en op hoeveel plekken het staat.
O	Oordeel	Wat betekent dit? Snelheid tegen zorgvuldigheid, indammen tegen doordraaien, open zijn tegen juridisch voorzichtig. Wie die afweging niet uitspreekt, maakt hem toch, alleen kan niemand hem later navertellen.	Welke afwegingen expliciet zijn gemaakt, en welke alleen impliciet.
B	Besluit	Wat gaan we eraan doen? Dit is waar de twintig tot veertig minuten verdwijnen. Er zit een zaal vol mensen die weten wat er moet gebeuren, en niemand die zeker weet of hij het mag laten doen.	Tijd tot het eerste besluit mét een eigenaar.
O	Opdracht	Wie gaat het doen? Een besluit dat geen opdracht wordt, is een mening. In de luchtvaart en de operatiekamer wordt een opdracht herhaald voordat hij wordt uitgevoerd; in een crisisruimte wordt hij meestal de zaal in gezegd.	Hoeveel besluiten een opdracht werden, en hoeveel bleven hangen.
C	Controle	Is het gedaan? Terugkijken hoort niet pas achteraf. Een opdracht die niet is nagekeken, is een aanname waarop de volgende drie besluiten rusten.	Hoeveel opdrachten zijn nagekeken voordat het beeld verschoof.
+	Overdracht	Wie neemt het over? Hier staat niets over in de modellen, en het gebeurt in elke lange crisis. Om middernacht wisselt de ploeg en verdwijnt wat niet is opgeschreven: de aannames, de openstaande opdrachten en de redenen waarom iets eerder is afgewezen.	Wat er verdwijnt bij de wissel, en hoe lang het herstel kost.

5. In OT is stilleggen een ander besluit

In een kantooromgeving is het zware besluit meestal: herstellen we nu, of bewaren we eerst bewijs. In een industriële omgeving komt er een besluit bij dat van een andere orde is, namelijk of de installatie door mag draaien.

Dat besluit is geen securitybesluit. Het raakt veiligheid, het raakt levering, en het ligt bij iemand anders dan de CISO. In de praktijk is dat de reden dat het blijft hangen: de securitykant durft het niet te nemen en de productiekant weet niet dat het aan hem is.

Daar komt bij dat de informatie waarop het besluit rust zelf verdacht is. Als procesdata niet meer te vertrouwen is, weet je niet of de installatie doet wat het scherm zegt. Beeldvorming is daarmee in OT geen verzamelstap maar een oordeel op zich.

Het spoor is hetzelfde, de inhoud van elke stap niet. Daarom oefenen wij OT en IT apart en niet met hetzelfde scenario in een ander jasje.

6. Wat je meet, en wat een score niet is

Elk van de zes stappen heeft één waarneming met een klok of een ja of nee eraan. Geen indruk van de begeleider, maar een tijd of een aantal. Dat maakt het navertelbaar en, belangrijker, herhaalbaar: dezelfde zes metingen in een volgende oefening laten zien of er iets is veranderd.

Nooit naast een naam. De uitkomst gaat over de keten, niet over een persoon. Een tijd die te lang was, zegt iets over de afspraak die ontbrak, en zelden iets over degene die stond te wachten.

En een goede uitslag is geen garantie. Een oefening is een oefening: de gevolgen zijn niet echt, de dag is gekozen en iedereen weet dat hij meedoet. Wat je meet is of de keten werkt onder omstandigheden die erop lijken, niet of hij houdt onder omstandigheden die het zijn.

7. Wat de wet hiervan vraagt

De Cyberbeveiligingswet legt een aantal dingen bij het bestuur neer. De maatregelen behoeven zijn goedkeuring (artikel 24, eerste lid), en ieder bestuurslid beschikt over kennis en vaardigheden om risico's te identificeren, maatregelen te beoordelen en de gevolgen daarvan voor de eigen dienstverlening te wegen (artikel 24, tweede lid). Dat moet binnen twee jaar na inwerkingtreding van dat lid (derde lid), aantoonbaar actueel blijven (vierde lid), en blijken uit een certificaat waaruit de deelname blijkt aan een training die die onderwerpen behandelt (vijfde lid).

Let op het woord deelname. De wet vraagt geen examen, geen accreditatie en geen erkend stelsel. Bij algemene maatregel van bestuur kunnen nog regels komen over de duur en het niveau van die training (zesde lid); die regels zijn er op het moment van schrijven niet.

Wanneer de klok begint te lopen staat niet in de wet. Artikel 107 laat de inwerkingtreding over aan een koninklijk besluit dat per artikel of per onderdeel kan verschillen. Wie beweert dat de termijn op een bepaalde datum is gaan lopen, beweert meer dan de wettekst draagt.

Daarnaast loopt bij een significant incident een klok van vierentwintig uur voor de vroegtijdige waarschuwing, en die begint bij bewustwording en niet bij begrip. Dat is een besluit onder onzekerheid, en het valt precies in de derde stap van dit spoor.

8. Grenzen van dit stuk

Dit is een praktijkstuk. Het spoor komt voort uit wat wij in crisisruimtes zien en uit bestaande werkwijzen, niet uit eigen onderzoek. Wij hebben niet aangetoond dat een korte tijd tot het eerste besluit samenhangt met een betere afloop van een echte crisis; dat zou vragen om waarneming tijdens echte crises, en die worden niet voor onderzoek ingericht.

De zes stappen zijn bovendien niet scherp van elkaar te scheiden. Beeld en oordeel lopen door elkaar, en controle levert een nieuw beeld op. Het spoor is een manier van kijken, geen natuurwet.

En het is de helft van het verhaal. De andere helft gaat over gedrag onder druk, en daarvoor zijn andere en betere stukken geschreven dan dit.

9. Slot

Een plan beschrijft wie welk besluit neemt. Een oefening laat zien of dat besluit ook genomen wordt, door wie, en wat ermee gebeurt daarna.

Het verschil tussen die twee is de reden dat oefenen niet te vervangen is door lezen. Niet omdat mensen het niet begrijpen, maar omdat een keten pas zichtbaar wordt als er iets doorheen moet.

Bronnen

Dit stuk leunt op de volgende werkwijzen en teksten. Het is een korte lijst met opzet: wat er onder ligt, en niet meer dan dat.

- Cyberbeveiligingswet, in het bijzonder de artikelen 21, 24, 26 en 107. Wettekst via wetten.overheid.nl.
- Richtlijn (EU) 2022/2555 (NIS2), via EUR-Lex.
- BOBOC, de werkwijze voor beeld-, oordeels- en besluitvorming met opdrachtverstrekking en controle, zoals gebruikt in de Nederlandse crisisbeheersing.
- Klein, G. A. (1993). A recognition-primed decision model of rapid decision making. Over beslissen met onvolledige informatie.
- Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Over beeldvorming als meer dan waarnemen.
- Weick, K. E. (1993). The collapse of sensemaking in organizations: the Mann Gulch disaster. Over wat er gebeurt als het gedeelde beeld instort.
- NCSC, kwetsbaarheden in PHP (CVE-2026-109618 en CVE-2026-109619), community.ncsc.nl/p/php, geraadpleegd 22 oktober 2026, en advisory NCSC-2026-0443.
- Mijndomein, statusmelding PHP-kwetsbaarheden, 21 en 22 oktober 2026.
- Terugkoppeling op een opdracht en gestructureerde overdracht zijn praktijken uit de luchtvaart en de zorg. Dit stuk gebruikt ze als werkwijze en doet geen uitspraak over de onderzoeksliteratuur erachter.