DISEM INSTITUTE

Een digitale veiligheidsstrategie

toekomst georiënteerd en gevalideerd

https://disem-institute.com/

Een digitale veiligheidsstrategie, *toekomst georiënteerd en gevalideerd*

De maatschappij is steeds meer onderhevig aan technologische ontwikkelingen en verdere digitalisering; ook op gebied van digitale veiligheid. Dit maakt de maatschappij steeds meer verweven, complexer en dynamischer. Hiermee komt er een terecht bestuurlijk vraagstuk: "in welke mate is de digitale veiligheidsstrategie toekomst bestendig is? " en "tegen welke kosten is het digitaal beveiligen acceptabel?". Het huidig, op het verleden gerichte, bestuurlijk instrumentarium van risico analyse, benchmarks en toetsen aan standaarden zal geen antwoord bieden. Disem Instituut heeft een toekomst gerichte aanpak die gegrond is in de wetenschappelijke methode van het dynamisch modelleren. Deze aanpak biedt (1) inzicht in de samenhang van complexe vraagstukken, (2) laat zien hoe een strategie zich in de toekomst gaat ontwikkelen en (3) geeft inzichten voor bijstelling en vervolg acties. Hiermee ontstaat strategische zekerheid over een digitale veiligheidsstrategie alvorens deze te implementeren.

Technologische ontwikkelingen en digitalisering

We leven vandaag de dag in een geavanceerde, digitale maatschappij, waarin de ontwikkelingen op technologisch gebied in rap tempo evident en manifest zijn. Krachtige, geavanceerde en snelle netwerken, forse toename van digitale apparaten en immer innovatieve, voortschrijdende automatisering is overal zichtbaar. Dit leidt tot merkbaar meer onderlinge verwevenheid en connectiviteit.

Ook beïnvloeden de technologische ontwikkelingen in toenemende mate ons dagelijks leven door middel van wearables, met apps verbonden huishoudelijke apparaten en snelle, mobiele technologie. Communicatie gaat in de 24/7-economie, zowel zakelijk en privé, in een toenemende mate via mobiele technieken, waarbij we voortdurend bereikbaar zijn. De stedelijke gebieden worden volledig digitaal via smart-city-concept. Voor bedrijven is er een fors groeiende toepassing van geautomatiseerde en gerobotiseerde procestechniek. Thans is met zeer hoge actualiteitswaarde, zelfdenkende, zelfredenerende en zelflerende programmatuur onstuitbaar in de ontwikkeling.

Zodoende ontstaat er een maatschappij die technologisch gezien, in onderling verband en samenhang meer en meer, verweven en verbonden is met een tijdfase van sterk opkomende, digitale, innovatieve ontwikkelingen. Daarbij zijn, juist vanwege die technologische innovatie, toenemende communicatie- en denkkracht potentieel aanwezig en in brede zin nuttig toepasbaar. Hierdoor

vinden (adequate, noodzakelijke en beslissende) activiteiten sneller of zelf automatisch plaats. Deze digitalisering is sterk actueel en geldt voor de gehele maatschappij. Juist en nadrukkelijk ook op het gebied van digitale veiligheid.

Met behulp van een wetenschappelijk gevalideerde methode zijn goede en adequaat-werkende strategieën, als ondersteuning voor strategisch management realiseerbaar. Evenzo is deze methode toepasbaar bij complexe, dynamische, maatschappelijke vraagstukken.

Complexiteit en dynamiek in digitalisering leiden tot een vraag van inzicht en begrip voor adequate besluitvorming.

Strategie, besturing en IT

Bestuurders van organisaties stellen zich frequent strategisch bezien de vraag: Hoeveel geld is te besteden aan digitale veiligheid? Immers, zij kunnen financiën maar één keer uitgeven. Alle budgetten die zij aan digitale veiligheid toekennen, zijn dus niet beschikbaar voor andere strategische bedrijfsactiviteiten. Hoewel de kosten voor digitale veiligheid duidelijk zijn, lijken de voordelen van het vermijden van mogelijke, potentieel-toekomstige, digitale aanvallen vaag, en ver weg.

Dit betekent dat gewoonlijk de besluitvorming terughoudend is om geld te investeren in een noodzakelijke, adequate, digitale veiligheidsstrategie. De mens is van nature risicomijdend en heeft een voorkeur voor zekerheid. De kosten voor goede digitale veiligheid vormen uitgaven die absoluut zekerheid zijn, terwijl de opbrengsten van die verdediging - wel of geen digitale aanval - toekomstig onzeker zijn. Men is dan geneigd om toch niet te investeren en vertoont risicomijdend gedrag. Daarnaast kan de focus van bestuurders onbedoeld afgeleid zijn door de symptomen, waardoor zij zich minder kunnen richten op moeilijk te observeren grondoorzaken. Hierdoor prevaleren bij hen de investeringen in andere, op dat moment belangrijker ogende strategische, bedrijfsactiviteiten. Voorbeelden zijn zoals: Een belangrijke marketingcampagne doorvoeren. Innovatie van de producten, services en processen. Een grote, unieke order binnenhalen. Websiteverbetering of een nieuwe locatie openen.

Hierdoor leiden die keuzes van vandaag, onbewust tot de problemen van morgen, mogelijk met desastreuse gevolgen voor reputatie, klantvertrouwen en de financiën. Toekomstige digitale veiligheidsincidenten leiden tot hoge kosten voor correctie en herstel voor organisaties. Wanneer een grote data breach zich acuut

manifesteert, wijzigen de prioriteiten direct en absoluut. In die onwenselijke crisissituatie heeft de verdedigende organisatie dubbele kosten, namelijk: de schade van de data breach herstellen en alsnog de investeringen in noodzakelijke, goede, digitale veiligheid. De voorbeelden hiervan zijn legio.

Bestuurders hebben behoefte aan duidelijk inzicht in korte en lange termijngevolgen van hun keuzes aangaande digitale veiligheid.

De dynamiek van digitale veiligheid

We proberen met de huidige, statische bestuurlijke middelen van risicomanagement, best practices, standaarden en benchmarks, onze digitale veiligheid te verbeteren. Die instrumenten leveren slechts een momentopname op. Zij geven inzicht in het 'nu'. Echter, de wereld is snel en veranderlijk. De inzichten van nu zijn morgen weer verouderd. Een digitale aanvaller geeft niet om een risico-inschatting; het regardeert hem totaal niet. De cybercrimineel boeit het niet of een organisatie compliant is. De dreigingsactor geeft niets om de reikwijdte van een veiligheidsfunctie ten opzichte van andere vergelijkbare organisaties. Aanvallers zijn op zoek naar zwakheden in de systemen, apparatuur, software, processen en kennis van de medewerkers om die te misbruiken voor geldelijk gewin of anderszins.

Er is een contante dynamische interactie tussen de aanvaller en de verdedigende organisatie, hierna de verdediger. Beide partijen zoeken naar zwakheden in processen, technologie en menselijk handelen. De aanvaller wil deze misbruiken en de verdediger wil dit uiteraard voorkomen. Die dynamiek, aanvallen en verdedigen, is zeer veranderlijk van aard en raakt zo de bedrijfsvoering en IT; kan forse, schadelijke gevolgen hebben voor de financiën en risicomanagement van de verdediger en beïnvloedt ook merkbaar de personele capaciteit. Echter, wanneer één van de partijen succesvol is met aanvallen of verdedigen, dan anticipeert de ander hierop en past haar werkwijze aan.

Bezien vanuit deze dynamiek betreft de digitale veiligheid vier sterk met elkaar verweven vraagstukken die het succes en de prestaties van de organisatie bepalen:

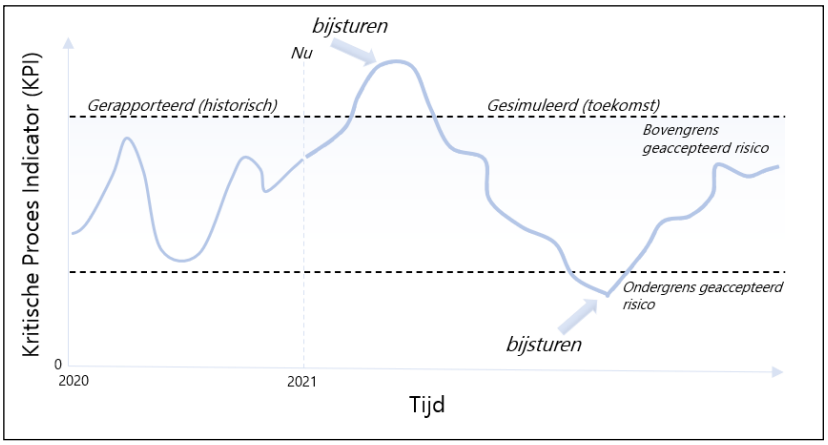
1. Het beheersen van de vaardigheden van verdedigen. Dit betreft de mate waarin de verdediger zwakheden kan signaleren en oplossen in medewerkerskennis,

processen, software en digitale apparaten om te voorkomen dat de aanvaller deze misbruikt.

2. Het vinden van de naald in de hooiberg. Dit gaat over de mate waarin de verdediger in staat is om te reageren op veiligheidsincidenten, die gefilterd zijn uit geobserveerde, verdachte signalen.
3. Het winnen van de inlichtingenrace. Dit is de mate waarin de verdediger in staat is om actief te leren van de ontwikkeling van de aanvaller.
4. Het beheren van de groei. Dit betreft de werkdruk die die verdediger aan kan, rekening houdend met het continueren van reguliere bedrijfsvoering, het implementeren van nieuwe, strategische ontwikkelingen en het mitigeren van incidenten.

Een verdediger kan door een succesvolle aanval enorm geconfronteerd worden met ingrijpende gevolgen van correctie en herstel. Vaak is dit causaal en indicatief te herleiden naar het ontoereikend invullen van de sterk met elkaar verwezen vier vraagstukken.

De dynamiek in digitale veiligheid heeft proactieve, vooruitkijkende risicomanagementinzichten nodig om de effectiviteit van (voorgenomen) besluiten te valideren.



Figuur 1. KPI-rapportage in een context van proactief risicomanagement.

Figuur 1 is een voorbeeld van proactief risicomanagement. Dit figuur laat zien dat op basis van toekomstige gesimuleerde uitkomsten besluitvormers nu al besluiten kunnen nemen ingeval de uitkomsten buiten de grenzen van het door het geaccepteerde risico zullen gaan komen.

Een valide digitale veiligheidsstrategie

Het klinkt als een cliché: de besluiten van vandaag leiden tot de problemen van morgen en, als je vooraf weet wat haalbaar is, hoef je achteraf niet veel te corrigeren. Organisaties kunnen het zich niet meer veroorloven om 'op goed geluk' te managen. Desondanks zijn veel organisaties onbedoeld miljoenen, mogelijk zelfs miljarden kwijt aan de kosten voor correctie en herstel. Besluitvormende processen in organisaties zijn complex en vergen geregeld veel tijd. Immers, er is een plan van aanpak nodig, een haalbaarheidsanalyse en een businesscase met financiële doorrekening. Veelal zijn bij organisaties meerdere specialismen of zelfs afdelingen betrokken met hun eigen methoden, beleidsregels en uitgangspunten. Pas nadat zo een plan goedgekeurd is, is implementatie mogelijk. Werving en selectie van personeel kost tijd. Hetzelfde geldt voor leveranciersselectie. Een doorlooptijd van maanden en soms jaren kan heel normaal zijn. De aanvaller heeft hier niet mee te maken. Hij heeft zijn eigen hogere ontwikkelsnelheid en flexibeler innovatiepatroon en wordt niet door vertraging in tijd gehinderd.

Hiermee is zichtbaar dat er een samenhang is tussen de structuur van een ecosysteem (lees: geheel van mensen, processen, technologie en besturing) en het gedrag van dit ecosysteem. Dit is basis van de systeem-gedrag-paradigma een belangrijk uitgangpunt bij het dynamisch modelleren.

Dynamisch modelleren is een wetenschappelijke methode die de inzicht biedt hoe de structuur van een onderliggend ecosysteem leidt tot bepaald gedrag en op welke wijze dit gedrag via besluitvorming kan worden beïnvloed. Deze methode biedt de mogelijkheid om dynamisch complexe vraagstukken te analyseren.

De basis om eerder genoemde problemen op te lossen ligt in het inzichtelijk maken van de interactie tussen de aanvaller en de verdediger en begrijpelijk te laten zien hoe die problemen vervolgens van invloed zijn bij klanten, reputatie en financiën. De mate waarin een organisatie kan reageren op de aanvaller is weer afhankelijk van de samenhang tussen medewerkers, processen, technologie en aansturing. Figuur 2 is voorbeeld van zo een structuur.

Figuur 2. Structuur ecosysteem.

De brug die Disem Institute slaat tussen wetenschap en de praktijk is bijzonder innovatief. Deze brug zorgt ervoor dat nieuwe analysemethodes, waaronder dynamisch modelleren, beschikbaar zijn. Disem Institute past de wetenschappelijk gevalideerde methode van dynamisch modelleren toe op het specialistische vakgebied van digitale veiligheid. Hierdoor kan Disem Institute duidelijk en begrijpelijk inzicht bieden in eerder genoemde interacties en samenhang. De aanpak van Disem Institute biedt met behulp van specifieke algoritmes de mogelijkheid om simulaties met toekomstprojecties te creëren en interventiepunten te identificeren. De wetenschappelijk gevalideerde aanpak van het dynamisch modelleren door Disem Institute, leidt tot duurzame en werkende strategieën die bestuurders inhoudelijk ondersteunen voor het voeren van goed bestuur. De innovatieve strategie resulteert waarneembaar in minder reparatie- en correctiekosten, omdat vooraf inzichtelijk is wat t.a.v. de digitale veiligheid strategie niet werkt en, in een eerder stadium krijgt de bestuurder duidelijk inzicht om bij te sturen.

De wetenschappelijk gevalideerde methode van dynamisch modelleren gebruikt door Disem Institute biedt inzicht hoe een voorgenomen digitale veiligheidsstrategie zich gaat ontwikkelen en laat vroegtijdig zien welke interventiemogelijkheden er zijn. Dit inzicht biedt bestuurders een solide en gedegen digitale veiligheidsstrategie.

Referenties

Kahneman D., 2011. Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011.

Kahneman D., & Tversky A., 1979. Prospect Theory: An Analysis of Decision Under Risk, Econometrica, 1979, Vol 47, No 2.

Moore T., Duynes S., & Chang F.R., 2016. Identifying How Firms Manage Security Investment. Workshop on the Economics of Information Security (WEIS), Berkeley, CA, June 13–14, 2016.

Paich, M., Peck, C. and Valant, J., (2009). Pharmaceutical product branding strategies: simulating patient flow and portfolio dynamics. Second edition. Informa Healthcare USA. Inc.

Paape L., 2008. 'In Control' statements: Fried air or a phenomenon to be cherished? Oration, Nyenrode Business Universiteit, 2008.

Zeijlemaker S., Bening R. & Rouwette E.A.J.A. (2019). Unravelling the dynamic complexity of cyber security investment decision making. In One Conference 2019. The Hague, the Netherlands

Zeijlemaker S., (2016). Exploring the dynamic complexity of the cyber security economic equilibrium. Colloquium of the 34th International Conference of the System Dynamics Society: Delft, the Netherlands (2016, July 17 - 2016, July 21).

Disem Institute

Disem Institute is gespecialiseerd in het analyseren van complexe, dynamische en strategische managementvraagstukken en excelleert op het gebied van digitale veiligheid. Disem Institute biedt de middelen om te zien en te volgen, hoe strategische beslissingen zich in de toekomst verklaarbaar zullen voordoen. Onze wetenschappelijk gevalideerde aanpak toont de effectiviteit van een strategie aan voordat bestuurders grote investeringen doen.