AUDIT
MAGAZINE

ARTIKELEN | 1 OKTOBER 2022

DE NOODZAAK VAN CYBER RESILIENCE

Auteur: Tekst: Jan Hendrikx MSc RE CISSP CISA CISM CRISC CIPPe
Beeld: Jeremy Bishop -Bernard Hermant - Kony
Leestijd: 7 min

Enkele jaren geleden deed, na cybersecurity, de term cyber resilience haar intrede. Hoewel deze termen vaak als synoniemen worden gebruikt, kennen de gebieden toch een groot verschil. In dit artikel ga ik op dit verschil in en belicht ik de noodzaak van cyber resilience. Ook leg ik uit hoe organisaties cyber resilience kunnen implementeren en hoe internal auditors het object cyber resilience kunnen toetsen.

Het Engelstalige woord resilience staat voor weerbaarheid, waardoor de term cyber resilience zich laat vertalen tot cyberweerbaarheid. Volgens het online Cybersecurity Woordenboekproject staat de term cyberweerbaarheid voor ‘het vermogen om (relevante) digitale risico’s tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken’. Maar hoe verhoudt cyber resilience zich dan ten opzichte van cybersecurity?

Verschil

Het verschil tussen cybersecurity en cyber resilience laat zich wellicht het best uitleggen aan de hand van de Security

Lifecycle uit het National Institute of Standards and Technology (NIST) Cybersecurity Framework (zie *figuur 1*).

Figuur 1. NIST Security Lifecycle

De NIST Security Lifecycle bevat securityfuncties die organisaties inrichten rondom securityincidenten. Cybersecurity focust zich daarbij vooral op de functies identify en protect terwijl cyber resilience zich ook focust op de functies detect, respond en recover. Dit maakt dat men bij cybersecurity met name bezig is met het in kaart brengen van de risico's die men als organisatie loopt (identify) en het voorkomen van cyberincidenten door het nemen van beschermende maatregelen (protect). Bij cyber resilience kijkt men ook naar de getroffen maatregelen om aanvallen te herkennen (detect), de wijze waarop men dergelijke aanvallen kan stoppen of afslaan (respond) en de manier waarop men weer zo snel mogelijk kan herstellen naar een niveau van dienstverlening dat acceptabel is (recover). Je zou cyber resilience daarom als een uitbreiding op de traditionele cybersecurity kunnen zien.

Noodzaak

Waarom moet u als organisatie iets met cyber resilience? In de eerste plaats moet het vanuit wet- en regelgeving. In artikel 32 van de Algemene Verordening Gegevensbescherming (AVG) staat dat de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen moeten treffen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen. Omdat zo goed als alle organisaties op de een of andere manier persoonsgegevens verwerken, ontkomt men er niet aan om iets aan cyber resilience te doen.

De kans is groot dat uw organisatie vroeg of laat wordt getroffen door een cybersecurityincident. Ook al patcht u zeer frequent uw systemen en doet u veel aan cybersecurity

Ook in de Wet beveiliging netwerk- en informatiesystemen (Wbni) voor onderdelen van het Rijk, digitale dienstverleners (DSP's) en aanbieders van essentiële diensten (AED's) staat een verwijzing naar de versterking van de digitale weerbaarheid. Om er achter te komen of uw organisatie onder de Wbni valt, kunt u de websites van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en van het CSIRT voor digitale dienstverleners (CSIRT-DSP) raadplegen.

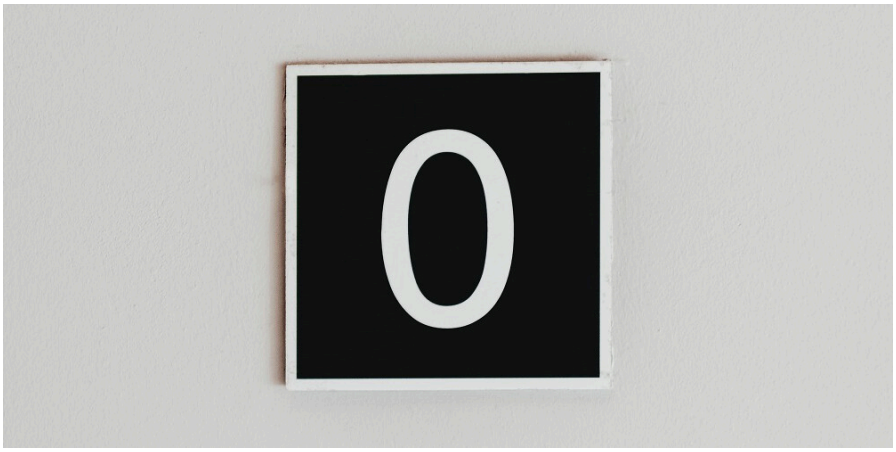
Intrinsieke reden

Hoewel voldoen aan wet- en regelgeving natuurlijk belangrijk is, is er een belangrijkere en wellicht meer intrinsieke reden om de cyberweerbaarheid op orde te hebben. De kans is namelijk groot dat uw organisatie vroeg of laat wordt

getroffen door een cybersecurityincident. Ook al patcht u zeer frequent uw systemen en doet u veel aan cybersecurity. Software bevat bijna van nature kwetsbaarheden en wordt naarmate het ouder wordt steeds kwetsbaarder. Dit komt omdat wanneer software veroudert, steeds meer mensen de software hebben kunnen onderzoeken op kwetsbaarheden. Vervolgens kan deze kennis uitlekken en worden misbruikt om kwetsbare systemen aan te vallen.

Zero-day

In veel gevallen worden er door softwareontwikkelaars updates uitgebracht om kwetsbaarheden te verhelpen, voordat deze kwetsbaarheden publiekelijk bekend worden. Maar in sommige gevallen zijn softwareontwikkelaars te laat en zijn er nog geen updates beschikbaar voor een kwetsbaarheid. Dit soort kwetsbaarheden worden zero-days genoemd (naar het aantal dagen dat de leverancier bekend is met de kwetsbaarheid in haar software). Afhankelijk van de ernst van een zero-day kan een aanvaller uw organisatie ernstige schade berokkenen.



Een voorbeeld van zo'n ernstige zero-day was de log4j-kwetsbaarheid die het voor aanvallers mogelijk maakte om systemen over te nemen. Deze kwetsbaarheid was relatief eenvoudig te misbruiken en was bovendien lastig te verhelpen, omdat log4j een generieke component is dat in veel verschillende soorten software is opgenomen. Organisaties moesten in hun eigen infrastructuur op zoek naar plaatsen waar log4j werd gebruikt en vervolgens wachten op een update voor hun specifieke software. Als een dergelijke update niet beschikbaar was, kon men proberen om de kwetsbare software zelf aan te passen of om andere maatregelen te nemen (zoals het tijdelijk isoleren van deze software). Vanwege het gemak waarmee de kwetsbaarheid in log4j te misbruiken was, werd er op grote schaal misbruik van gemaakt. Zero-days komen niet alleen in amateuristische software voor, ook in softwareproducten van de grote en bekende leveranciers worden ze regelmatig ontdekt.

Implementeren

Hoe kan men als organisatie cyber resilience nu implementeren? In veel van de populaire security frameworks en normenkaders zitten elementen die cyber resilience raken. Maar deze elementen zijn vaak versnipperd en soms niet zo gemakkelijk te herkennen. Het NIST Cyber Security Framework biedt gelukkig een oplossing. Het framework is te downloaden van de NIST-website en bevat een handige toelichting met hoe het framework te gebruiken. Hoewel het framework op meer zaken ingaat dan weerbaarheid, wil ik me focussen op de Framework Core dat is ondergebracht in Appendix A. Deze appendix bevat een tabel die een opsomming van cybersecurity en -weerbaarheidactiviteiten geeft en die men verwacht aan te treffen bij AED's.

Wanneer u de voordelen van dit framework kent, hebt u eigenlijk geen goed excuus meer om niets te doen aan cyber resilience

Functies

De tabel bevat aan de linkerzijde de eerdergenoemde functies uit de Security Lifecycle met in de volgende kolom bijbehorende beheersdoelstellingen, zogenaamde ‘categories’. Deze zijn in de volgende kolom weer opgesplitst in beheersmaatregelen, de ‘subcategories’. Ten slotte zijn deze subcategories gemapped op de relevante beheersmaatregelen uit een aantal bestaande populaire security frameworks, zoals CIS en COBIT.

De tabel maakt het mogelijk om per functie (identify, protect, detect, respond en recover) gericht de cybersecurity en -weerbaarheid in de eigen organisatie te versterken. Dit kan men doen door de (sub)categorieën te implementeren. Indien u al gebruikmaakt van een van de security frameworks wordt door de mapping inzichtelijk waar u mogelijk al cyberweerbaarheidsmaatregelen heeft getroffen. Ook kan men op basis van de mapping in de laatste kolom ideeën opdoen door te kijken welke resilienceactiviteiten horende bij dezelfde subcategorie in de andere frameworks worden beschreven.

Op deze manier wordt het mogelijk om een reeds geïmplementeerde subcategorie te verbeteren. Men kan zelf bepalen in welke volgorde men het Cyber Security framework wil implementeren en men is vrij om de tabel uit te breiden met nieuwe (sub)categorieën. Verder zijn de genoemde frameworks in de laatste kolom een suggestie, geen verplichting.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· CIS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· CIS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 · NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· CIS CSC 12 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· CIS CSC 12 · COBIT 5 APO02.02, APO10.04, DSS01.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	· CIS CSC 13, 14 · COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· CIS CSC 17, 19 · COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Tabel 1. Fragment uit de Framework Core

In *tabel 1* is de onderverdeling zichtbaar van de categorie ‘Asset management’ die valt onder de functie ‘Identify’.

U vraagt zich nu wellicht af: hoe bruikbaar is het NIST Cyber Security Framework voor mijn organisatie? Het framework kent de volgende voordelen:

- het is gratis;
- het past op ieder type organisatie van iedere omvang;
- het is een aanvulling op de bestaande populaire frameworks;
- men kan zelf kiezen welke (sub)categorie op welk moment wordt geïmplementeerd;
- afhankelijk van uw risk appetite kunt u (sub)categorieën achterwege laten.

Wanneer u de voordelen van dit framework kent, heeft u eigenlijk geen goed excuus meer om niets te doen aan cyber resilience.

Auditen

Hoe audit u nu de effectiviteit van de cyberweerbaarheid van uw organisatie? Traditionele audittechnieken kijken vaak alleen naar specifieke beheersmaatregelen, maar niet naar het geheel van die maatregelen. En hoe toetst men de werking van cyberweerbaarheidgerelateerde beheersmaatregelen? Het antwoord op deze vragen is dat u als internal auditor beoordeelt in hoeverre uw organisatie zogenaamde ‘red teaming’ toepast.

Red teaming

Red Teaming is een term die afkomstig is uit de Amerikaanse defensie. Tijdens red teaming testen militaire eenheden elkaars zwakheden door gesimuleerde aanvallen op elkaar uit te voeren. Daarbij is het rode team de aanvallende en het blauwe team de verdedigende eenheid. In de context van cyberweerbaarheid komt dit neer op een gesimuleerde cyberaanval. Vaak bestaat het rode team uit een groep securityspecialisten van een externe partij die worden ingehuurd om een gecontroleerde aanval uit te voeren. Het blauwe team bestaat uit medewerkers van de eigen organisatie. Meestal is het zo dat het blauwe team niet wordt geïnformeerd over wanneer de aanval door het rode team plaatsvindt. Dit zorgt ervoor dat het blauwe team altijd alert moet zijn. Het belangrijkste doel van red teaming is om ervan te leren. Overigens bestaat er naast het red en blue team ook nog een white team. In dat team zitten de mensen binnen de organisatie die de cyberaanval organiseren.

Mystery guests

Bij red teaming wordt de aanval over een langere periode uitgevoerd en kan het volledige aanvalsoppervlak van een organisatie worden getest. Daarbij wordt niet alleen de techniek getest, maar ook de menselijke factor. Denk daarbij aan het inzetten van mystery guests en phishingaanvallen om op die manier toegang te krijgen tot de organisatie.

Het is de bedoeling dat het rode team probeert zo ver mogelijk de technische infrastructuur van de organisatie binnen te dringen. Het witte team monitort of het blauwe team de aanval detecteert, of het in staat is om de aanvallen af te slaan en de dienstverlening kan herstellen. Hierbij zorgt het witte team dat de buitenwereld op tijd wordt gewaarschuwd dat er sprake is van een gesimuleerde aanval. Dat is belangrijk omdat het blauwe team niet weet of het om een test of een werkelijke cyberaanval gaat en daarom misschien de politie of het CSIRT inschakelt.

Het is de bedoeling dat het rode team probeert zo ver mogelijk de technische infrastructuur van de organisatie binnen te dringen

Na de aanval schrijft het rode team een rapport met daarin de bevindingen van de aanval. Deze rapportage kan door de auditors van de organisatie gebruikt worden om de staat van de cyberweerbaarheid te beoordelen. De bevindingen uit het rapport kunnen vervolgens gebruikt worden om de cyberweerbaarheid van de organisatie te verbeteren.

Sectorale initiatieven

Inmiddels zijn er al verschillende sectorale initiatieven gelanceerd hoe red teaming testen uit te voeren. Het bekendste initiatief is misschien wel het Threat Intelligence Based Ethical Red Teaming framework (TIBER-NL) dat afkomstig is van De Nederlandsche Bank (DNB). Dit initiatief is inmiddels overgenomen door de Europese Centrale Bank (ECB) die de red-teamingtesten bij financiële instellingen in Europees verband coördineert. De opgedane kennis wordt vervolgens binnen de sector gedeeld, zodat financiële instellingen aan de hand van deze kennis hun weerbaarheid kunnen vergroten. Ook de Nederlandse overheid onderschrijft het nut van red teaming. Uit antwoorden op Kamervragen blijkt dat red-teamingtesten ook binnen de Rijksoverheid worden toegepast.

Conclusie

Het is dus belangrijk dat uw organisatie aan de slag gaat met het vergroten van de cyberweerbaarheid. Het is waarschijnlijk een kwestie van tijd voordat ook uw organisatie wordt getroffen door een succesvolle cyberaanval. Dan is het goed wanneer u dit op tijd in de gaten hebt, u de aanval kunt afslaan en uw dienstverlening zo spoedig mogelijk weer kunt hervatten.

Over
Jan Hendrikx MSc RE CISSP CISA CISM CRISC CIPPe is ondernemer op het gebied van technische informatiebeveiliging. Hij voert technische beveiligingsonderzoeken uit en adviseert organisaties over de wijze waarop zij hun beveiliging tegen onder meer cybercriminaliteit kunnen optimaliseren.

Tags: Cyber resilience

Bron url: https://auditmagazine.nl/artikelen/de-noodzaak-van-cyber-resilience/