Cyberrisico's rapporteren aan raden van bestuur

Bestuursuitgave

Auteurs
Freddy Dezeure
George Webster
Lokke Moerel

Reviewers
Alan Kessler
Jamie Hutchinson

Datum: 14 maart 2022
Versie: Definitief

Doel

In dit document wordt een overzicht gegeven van de aanbevolen aanpak voor raden van bestuur bij het aanpakken van cyberrisico's, en van goede uitgangspunten voor de cybermetriek van raden van bestuur. Het is een aanvulling op een document dat is gericht aan Chief Information Security Officers (CISO's) over hoe zij cyberrisico's het beste kunnen controleren, meten en rapporteren aan hun Raad van Bestuur, en moet in samenhang met dat document worden gelezen.

De meeste raden van bestuur zijn niet cyberbewust

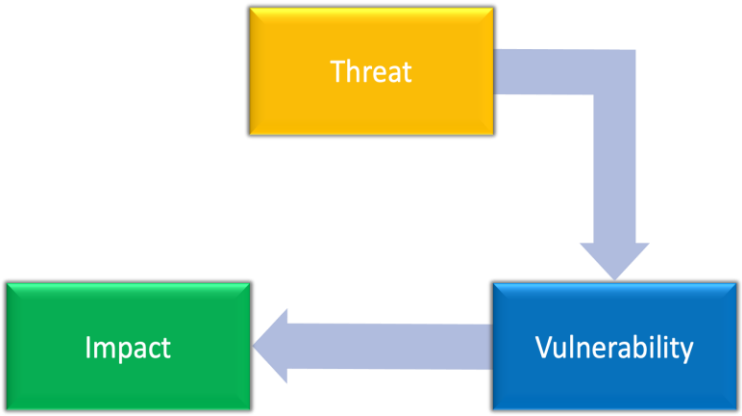
Raden van bestuur hebben een wettelijke plicht om goed toezicht te houden op risico's. Cyberrisico's vormen inmiddels een kritiek, potentieel materieel bedrijfsrisico. De meeste raden van bestuur zijn echter slecht toegerust om met cyberrisico's om te gaan. Ze beschouwen cyber als te technisch, keuren slechts middelen goed en delegeren het risico.

Voor traditionele bedrijfsrisico's bestaat er een gevestigde praktijk van hoe informatie moet worden gemeld en een aanvaarde verdeling van verantwoordelijkheid/delegatie. Voor cyberrisico's bestaat die momenteel niet. CISO's hebben moeite om de effectiviteit van hun cyberbeveiligingsprogramma te meten en redelijke zekerheid te verschaffen dat het resterende cyberrisico onder de risicobereidheid van het bedrijf blijft. Veel CISO's spreken geen "bestuurstaal" en worden niet uitgenodigd om verslag uit te brengen.

In uitzonderlijke gevallen waarin verslaglegging over cyberrisico's aan de Raad van Bestuur plaatsvindt, is er een grote verscheidenheid aan methoden, instrumenten en processen in gebruik. Vaak gaat de rapportage over de voortgang bij de uitvoering van cyberbeveiligingsmaatregelen (het meten van *de inspanningen*, waarbij vaak alles groen wordt gerapporteerd), in plaats van de rapportage over *risicovermindering*.

Het gaat allemaal om risico

Onze cyberomgeving dwingt ons keuzes te maken met betrekking tot wat te beschermen en hoe. Perfecte beveiliging is een illusie en de middelen zijn schaars. Beoordeling en beslissingen over prioriteiten worden vergemakkelijkt en geobjectiveerd door gebruik te maken van risicobeoordeling. Voor cyber gebruiken wij een model waarin risico is samengesteld uit drie factoren **Dreiging**, **Kwetsbaarheid** en **Impact**.



Figuur 1 Risico als een combinatie van dreiging, kwetsbaarheid en impact

Dreiging is meestal extern aan onze organisatie en is nauw verbonden met tegenstanders die onze organisatie schade zouden kunnen berokkenen. Het identificeren van onze **belangrijkste tegenstanders** en hun motieven is belangrijk voor het prioriteren van onze risicobeperkende maatregelen. Wij kunnen huidige dreigingen observeren en proberen toekomstige dreigingen te voorspellen.

De tweede factor is **kwetsbaarheid**, en dit is de factor waarop wij de meeste invloed kunnen uitoefenen door het ontwerpen en uitvoeren van controles en risicobeperkende maatregelen. Het identificeren van **de belangrijkste controles**, het in aanmerking nemen van onze belangrijkste activa en de motivatie en methoden van onze belangrijkste tegenstanders is belangrijk voor het stellen van prioriteiten.

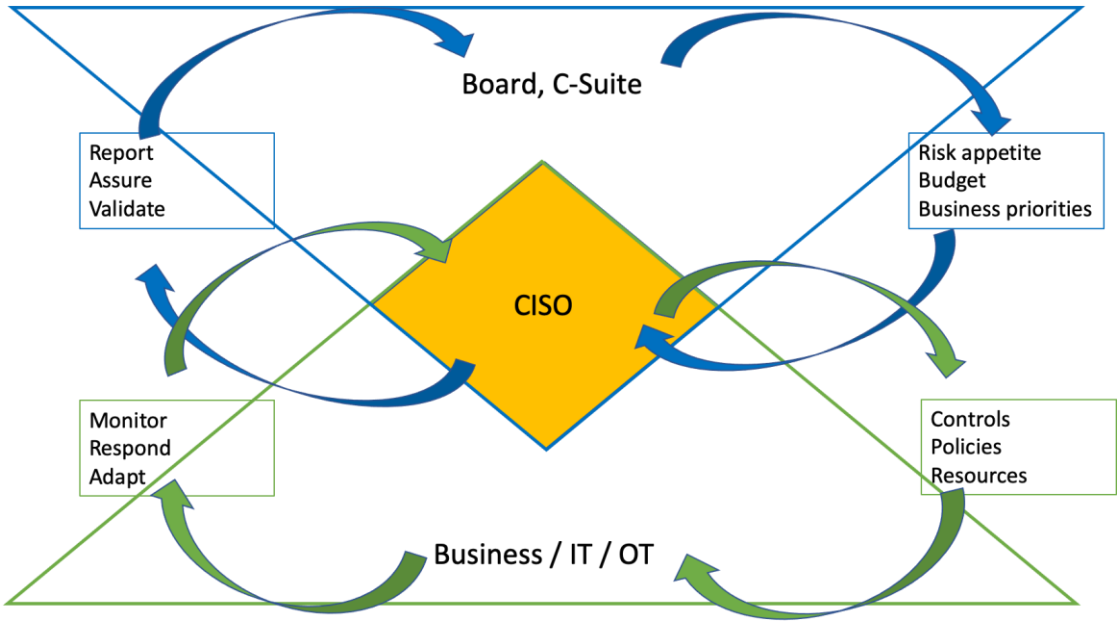
In termen van **impact** kunnen we denken aan diefstal van intellectueel eigendom, lekken van privégegevens, onderbreking van de dienstverlening, persoonlijke schade en reputatieschade. Impact is nauw verbonden met activa. Het identificeren van onze **belangrijkste activa** is belangrijk voor het stellen van prioriteiten.

Aanbevolen aanpak voor raden van bestuur

1. Cyberbewust worden en redelijke zekerheid verkrijgen

Verzoek om regelmatige rapportage en niet alleen in geval van een incident. Bevorder serieuze rapportage en niet alleen "alles duidelijk". Dring aan op interne afstemming en duidelijke communicatiekanalen, waarbij de CISO een centrale rol speelt en zorgt voor een professionele en onafhankelijke kijk op het cyberrisico[1].

[1] Informatiestromen, geïnspireerd door het NIST Cyber Security Framework https://www.nist.gov/cyberframework



Figuur 2 Informatiestromen en coördinerende rol van de CISO.

Het rapporteren van cyberrisico's moet dienen om de Raad van Bestuur (opnieuw) te verzekeren dat het risico vandaag en morgen binnen de risicobereidheid valt:

- Zijn we goed genoeg?
- Zijn de voor cyber toegewezen middelen adequaat en doeltreffend?
- Hoe verhouden wij ons tot onze collega's en onze sector?

De gerapporteerde cijfers kunnen worden gecombineerd met context over belangrijke incidenten binnen en buiten de onderneming, over dreigingen en ontwikkelingen in de regelgeving. De CISO moet alle ontwikkelingen signaleren die de situatie ten goede of ten kwade ingrijpend veranderen en als gevolg daarvan relevante acties en middelen voorstellen.

Een voorbeeldverslag ter illustratie van een mogelijke rapportagestructuur met voorbeeldcijfers is opgenomen in de bijlage.

2. De juiste situationele vragen stellen

De vragen die raden van bestuur aan hun CISO moeten stellen, houden nauw verband met de risicofactoren.

- Hebben we een inventaris van de belangrijkste activa?
- Wat voor soort tegenstanders hebben het op ons gemunt en waarom?
- Wat zijn onze belangrijkste controles en wat is hun status?
- Waar zitten de lacunes en hoe denken wij die te dichten?
- Hebben we een plan voor respons op incidenten / bedrijfscontinuïteit / veerkracht?
- Hoeveel staat er op het spel?
- Hoe verhouden wij ons tot onze sectorgenoten?

3. Uw risico's beheersen

Cyberbeveiligingsraamwerken zijn een hulpmiddel om cyberbeveiligingsrisico's op een samenhangende manier te beheren en om een bedrijfsstrategie voor

cyberbeveiliging uit te voeren. Veel gebruikte raamwerken zijn ISO/IEC 27001[2] en het Cyber Security Framework van NIST.[3] Het maakt niet veel uit welk raamwerk een organisatie kiest, omdat er koppelingen tussen de raamwerken zijn. Voor raden van bestuur is het wel belangrijk dat er volledige interne afstemming is (tussen CISO, IT/OT, en risicomanagement) over welk raamwerk door de organisatie wordt gebruikt.

Raamwerken bevatten doorgaans honderden controles waarover onmogelijk op het niveau van de Raad van Bestuur kan worden gerapporteerd. Daarom moeten de belangrijkste controles worden geïdentificeerd. Een goede plaats om te beginnen zijn de richtlijnen die door de verschillende nationale cyberbeveiligingsautoriteiten zijn uitgevaardigd. Er is een grote mate van overlapping tussen deze verschillende sets van basisrichtlijnen en ze bieden een uitstekend, beknopt en praktisch startpunt. Hieronder volgen enkele van de belangrijkste controles die er steevast in zijn opgenomen:

- K1: Een actuele inventaris bijhouden van alle (essentiële) activa en afhankelijkheden;
- K2: Betrouwbare, geldige, veilige en beveiligde back-ups maken van belangrijke activa;
- K3: Waar mogelijk afdwingen van multi-factor authenticatie;
- K4: Beperken van de toegangsrechten van gebruikers tot het strikt noodzakelijke;
- K5: Identificeren en tijdig patchen van belangrijke kwetsbaarheden;
- K6: Verzamelen en analyseren van logs van alle (belangrijke) activa;
- K7: Segmenteren van het netwerk om belangrijke activa te beschermen;
- K8: Verharden van systemen die op internet gericht zijn;
- K9: Een incidentenrespons- en herstelproces implementeren;
- K10: Bewustmaken van de gebruikers (met inbegrip van de leden van de Raad van Bestuur).

De beperking van elke controle zou kunnen worden gemeten en gerapporteerd aan de hand van een "dekkingsscore", waarin de inzet, de werking en de doeltreffendheid van een controle worden gecombineerd.

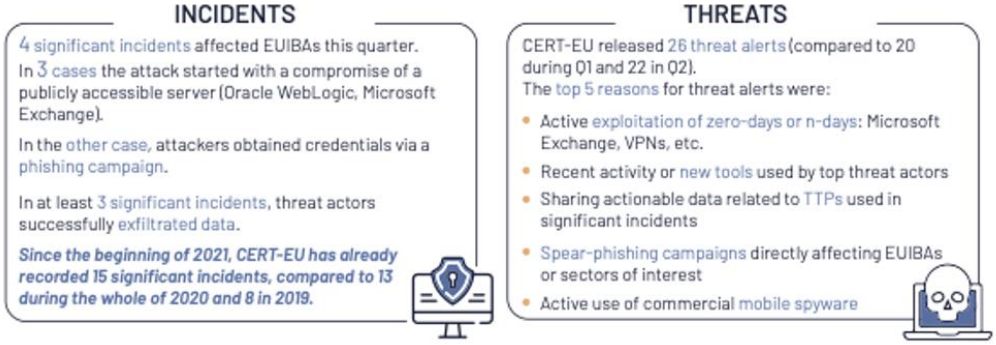
[2] https://www.iso.org/isoiec-27001-information-security.html
[3] https://www.nist.gov/cyberframework

Bijlage: Voorbeeld van een verslag

Ontwikkeling van het dreigingslandschap

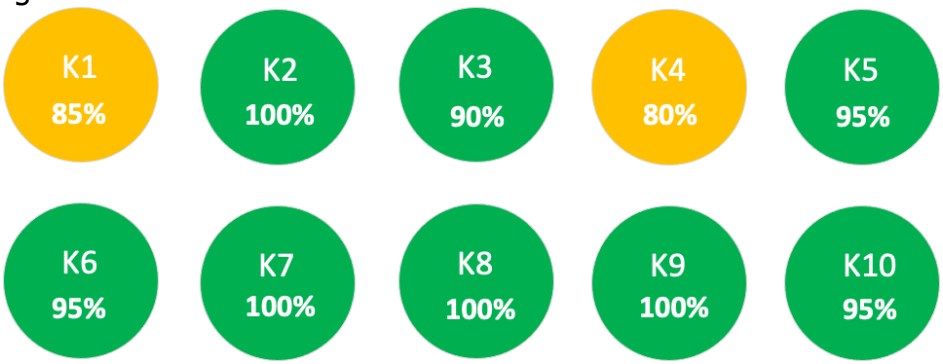
Who?	Group / Malware?	Why?	Trend
Adversary 1	APTX	Adversary known to steal intellectual property in high tech industry.	→
Adversary 2	APTY	State sponsored actor known targeting critical infrastructure	↗
Adversary 3	FINX	Ransomware actor increasingly prevalent and sophisticated	↗

Opmerkelijke ontwikkelingen in incidenten en dreigingen

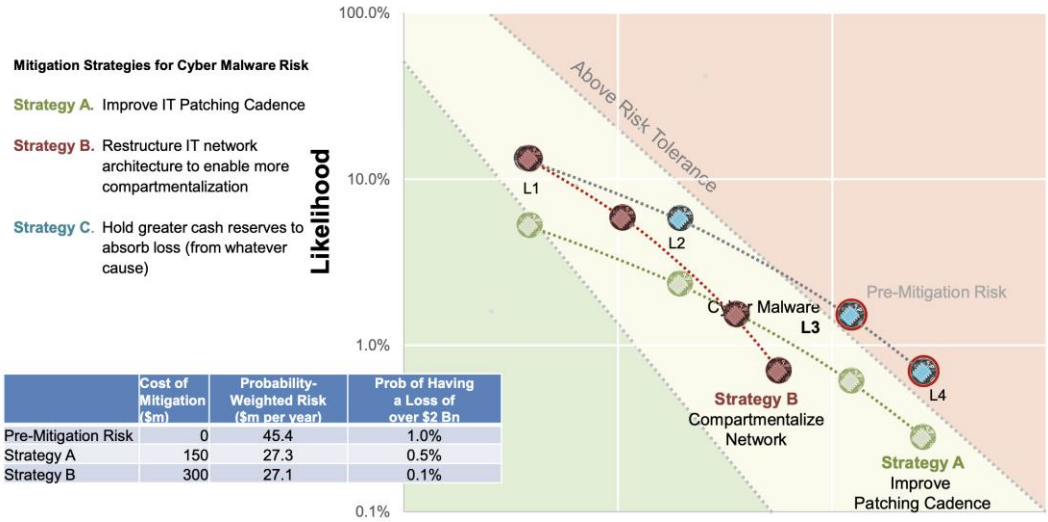


3 Krediet CERT-EU

Dekking van essentiële controles



Impact van aanvullende maatregelen op de beperking van het cyberrisico



	Cost of Mitigation ($m)	Probability-Weighted Risk ($m per year)	Prob of Having a Loss of over $2 Bn
Pre-Mitigation Risk	0	45.4	1.0%
Strategy A	150	27.3	0.5%
Strategy B	300	27.1	0.1%

Figuur 4 Kredietcentrum voor risicostudies, Universiteit van Cambridge