Zehn wichtigen Erkenntnisse für eine fundierte Cyber-Übersicht

Article · August 2023

CITATIONS
0

READS
11

8 authors, including:

Freddy Dezeure
Freddy Dezeure BV
26 PUBLICATIONS **3** CITATIONS
SEE PROFILE

João Pedro Gonçalves
EQT Group
14 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Eireann Leverett
Concinnity Risks
26 PUBLICATIONS **92** CITATIONS
SEE PROFILE

Lokke Moerel
Tilburg University
38 PUBLICATIONS **89** CITATIONS
SEE PROFILE

Berichterstattung zu Cyber-Risiken an Vorstände

Zehn wichtigen Erkenntnisse für eine fundierte Cyber-Übersicht

Autoren
Freddy Dezeure
Peter Debasse
João Pedro Gonçalves
Tristan Guiheux
Éireann Leverett
Patrick Mana
Lokke Moerel
Bartosz Sygula

Rezensenten
Greg Bell
Paolo Borghesi
Philippe Coffyn
Chris Deverell
Tom Gilis
Kevin Holvoet
Angelos Keromytis
Ed Millington
Dimitri Rombaut
Sam Singer

Datum: 30. August 2023
Version: final

Inhalt

Einführung

Im März 2022 haben wir das Weißbuch Berichterstattung über Cyber-Risiken an Vorstände veröffentlicht, das Chief Information Security Officers (CISOs) bei der Entwicklung und Umsetzung quantitativer Metriken für die Cybersicherheit unterstützt, um auf Vorstandsebene über Cyberrisiken zu berichten und hinreichende Gewähr dafür zu bieten, dass das Cyberrisiko innerhalb der akzeptierten Risikobereitschaft liegt. Das Weißbuch hat in der Community viel Aufmerksamkeit und Anerkennung gefunden und wurde weithin verbreitet. Das White Paper wurde auch in einer gekürzten Fassung für Verwaltungsratsmitglieder veröffentlicht.

Seit der Veröffentlichung des Weißbuchs haben zusätzliche aufsichtsrechtliche Anforderungen in der EU (NIS2[1] , DORA[2]) und den USA (SEC[3] , NYDFS[4]) die Verantwortung und Rechenschaftspflicht der Vorstandsmitglieder für eine sorgfältige und sachkundige Überwachung der Cyberrisiken in ihren Organisationen erhöht. Cyberrisiken spielen auch in der ESG-Berichterstattung eine immer größere Rolle. Einige dieser regulatorischen Anforderungen beziehen sich ausdrücklich auf Cyber-Metriken (DORA, Artikel 6). Derzeit gibt es noch keine offiziellen Leitlinien dazu, was eine ordnungsgemäße Aufsicht durch die Leitungsorgane darstellt, geschweige denn, welche strategischen Metriken dann zu einer *fundierten* Aufsicht führen könnten.

Rückmeldungen aus der Gemeinschaft zum Inhalt des Weißbuchs und zusätzliche Erkenntnisse haben gezeigt, dass ein Bedarf an zusätzlichen Leitlinien besteht, um die wichtigsten Erkenntnisse hervorzuheben und ihre Formulierung zu straffen. Das vorliegende Papier soll diesem Zweck dienen. Es enthält auch die Elemente, um die zusätzlichen regulatorischen Anforderungen hinsichtlich Information und Aufsicht des Verwaltungsrats zu erfüllen.

Dieses Papier baut auf dem grundlegenden Gedanken auf, dass ein solides Cyber-Risikomanagement *evidenzbasiert* sein sollte, anstatt sich auf Absichten oder Annahmen zu verlassen (die häufig auf Selbstauskünften beruhen). Strategische Cyber-Metriken sind ein wesentlicher Bestandteil jeder erfolgreichen Bemühung, Cyber-Risikomanagement zu priorisieren und umzusetzen.

Die Messung von Cybersicherheitsrisiken in *quantifizierbarer* Form unter Verwendung von Daten aus der Infrastruktur ist in der Branche noch nicht weit verbreitet. Es überrascht nicht, dass es auch keine einheitlichen Maßstäbe für einen Vergleich mit anderen Unternehmen gibt.

Das vorliegende Papier soll 10 wichtige Erkenntnisse von Unternehmen vermitteln, die strategische Cyber-Metriken eingeführt haben, damit die Gemeinschaft auf diesen Erkenntnissen aufbauen und sie in ihrem eigenen Umfeld anwenden kann. Die Erkenntnisse werden in klaren und zum

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555 (Artikel 20 und 21)
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554 (Artikel 5 und 6)
[3] https://www.sec.gov/news/press-release/2023-139
[4] https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf

Nachdenken anregenden Zusammenfassungen zusammengefasst, um die Übernahme zu erleichtern.

Dieser Ansatz mag als Verallgemeinerung oder Vereinfachung erscheinen, aber er wird dazu beitragen, die Aufmerksamkeit von CISOs und Vorständen zu straffen und zu fokussieren und letztendlich bessere Ergebnisse beim Management und der Überwachung von Cyberrisiken zu erzielen.

Das vorliegende Papier ist als Ergänzung zum Weißbuch aus dem Jahr 2022 zu sehen und es wird dringend empfohlen, beide zusammen zu lesen.

Zehn wichtige Erkenntnisse

1. Beweise statt Konformität

Viele Organisationen haben einen Cybersicherheitsrahmen (NIST, ISO, CIS) eingeführt oder befolgen spezifische Vorschriften und Normen (PCI-DSS, Solvency/Basel II), kombiniert mit externen Prüfungen und Zertifizierungen. Dies ist oft eine Voraussetzung für ihre Tätigkeit, sei es aus regulatorischen oder geschäftlichen Gründen (Versicherungen, Kunden). Dieser Ansatz sollte jedoch eher als Grundvoraussetzung denn als Allheilmittel betrachtet werden. Er gibt Normen und Richtlinien vor, die einzuhalten sind, spiegelt aber nicht unbedingt die tatsächliche Zweckmäßigkeit für die spezifischen Geschäftsrisiken wider.

Sind die vereinbarten Kontrollen ausreichend, um bei korrektem Funktionieren zu einer wirksamen Risikominderung zu führen? Werden sie vollständig eingesetzt? Funktionieren sie wie vorgesehen?

Die Organisationen mit hohem Reifegrad nutzen (kontinuierliche) Nachweise aus ihrer Infrastruktur, um die Wirksamkeit ihrer Kontrollen zu ermitteln, anstatt sich auf menschliche Beurteilungen, Selbstauskünfte und einmal im Jahr ausgefüllte Fragebögen zu verlassen. Die erforderliche Datenerfassung und -aufbewahrung stellt zugegebenermaßen eine große Herausforderung für diese Organisationen dar, sind aber der Ansicht, dass sich der Aufwand lohnt. Ein professionelles Urteilsvermögen kann weiterhin eine Komponente bei der Erstellung von Berichten an den Vorstand sein, wenn es durch Metriken aus operativen Datenquellen und Sicherheitstools untermauert wird.

2. Berichterstattung über KCIs statt über alles

Die Vorstände wollen einen Überblick über das, was wichtig ist, und nicht alle Kontrollen in Cybersicherheitsrahmenwerken sind gleich wichtig. Die meisten Rahmenwerke weisen darauf hin, dass eine begrenzte Anzahl von Kontrollen den größten Einfluss auf die Risikominderung hat.

Die Berichterstattung an den Vorstand über die wichtigsten Kontrollindikatoren (Key Control Indicators, KCIs) und ihre Entwicklung im Laufe der Zeit ist daher sinnvoller als die Berichterstattung über alle Kontrollen. Das bedeutet nicht, dass der CISO alle anderen Kontrollen aus den Augen verliert, aber es zeigt deutlich, was zu einem bestimmten Zeitpunkt die größte Wirkung bei der Risikominderung für eine bestimmte Organisation hat.

Verwechseln Sie das Konzept der Key Performance Indicators (KPIs) nicht mit KCIs. Ein CISO sollte an der Leistung seines Teams interessiert sein, aber KPIs sind nicht immer relevant dafür, wie gut das Cyber-Risiko eingedämmt wird. Die Berichterstattung des Verwaltungsrats erfordert strategische Indikatoren, die für das gesamte interne Umfeld repräsentativ sind und die Risikobereitschaft des Unternehmens untermauern. Detaillierte Anleitungen zu KCIs, ihrer Wirksamkeit und ihrem Erfassungsbereich finden Sie im Weißbuch Berichterstattung über Cyber-Risiken an Vorstände.

Hier finden Sie eine Beispielliste von KCIs als Ausgangspunkt:

KCI 1	Anlageninventar [5]	% der Vermögenswerte im Inventar innerhalb der Richtlinie
KCI 2	Privilegierte Konten	% privilegierte Konten, die im Rahmen der Richtlinie verwaltet werden
KCI 3	Rechtzeitiges Patchen	% Hochrisikopatches innerhalb von N Stunden # Anzahl bekannter ausgenutzter Schwachstellen entdeckt
KCI 4	Back-up	Maximale Zeit für die Wiederherstellung wichtiger Vermögenswerte (% der kritischen Vermögenswerte, die in N Stunden wiederhergestellt werden können)
KCI 5	Endpunktschutz	% Endpunkte, die entsprechend der Richtlinie konfiguriert sind
KCI 6	Sammlung von Protokollen	% kritische Systeme, die in die Protokollerfassung einbezogen sind
KCI 7	Sicherheit im Netz	%-konforme Konfigurationen der kritischsten netzsicherheitsrelevanten Systeme
KCI 8	Einhaltung der Vorschriften durch Dritte	% Policy konforme, wichtige Verbindungen zu Dritten
KCI 9	Identitätsmanagement	Erfassungsgrad der Systeme mit MFA in %
KCI 10	Größere Zwischenfälle	% größere Cyber-Vorfälle mit Auswirkungen auf das Geschäft
KCI 11	Risikoakzeptanz	# Abweichungen, deren Risiko akzeptiert wird
KCI 12	Sicherheit der im Internet exponierten Vermögenswerte	% der dem Internet ausgesetzten Systeme, die von der Sicherheitsüberwachung und regelmäßigen Sicherheitsbewertungen erfasst werden
KCI 13	Abdeckung der Kronjuwelen	% der Kronjuwelen, die durch Sicherheitsüberwachung, Schwachstellenscans und regelmäßige Sicherheitsbewertungen abgedeckt sind
KCI 14	Ursprung von Sicherheitsvorfällen	% der Sicherheitsvorfälle im Zusammenhang mit dem Versagen von mindestens einem KCI

3. Bedrohungsinformiert statt altbacken

Die Bedrohungslandschaft entwickelt sich weiter, und das sollten auch unsere Kontrollen und KCIs tun. Die Angreifer passen ihre Taktiken und Techniken an, um unsere Verteidigungsmaßnahmen zu umgehen. Sie wissen oft besser über unsere Infrastruktur und Kontrolllücken Bescheid als wir selbst. Sie überwachen die Offenlegung von Schwachstellen durch die Hersteller und reagieren darauf mit einer kürzeren Vorlaufzeit als wir. Einige verfügen über ausreichende Ressourcen, um ausgeklügelte Sicherheitslücken zu kaufen.

[5] Ein genaues und vollständiges Anlageninventar ist von entscheidender Bedeutung, da es den Nenner für viele der KCIs darstellt

Um negative Auswirkungen auf unser Geschäft zu vermeiden, müssen wir unsere Kontrollen an die Bedrohung anpassen und dabei unser spezifisches Umfeld und unsere Anlagen berücksichtigen. Dies erfordert ein Verständnis der Taktiken, Techniken und Verfahren des Gegners, eine Priorisierung und Neuausrichtung der Kontrollen sowie eine kontinuierliche Überwachung auf Anzeichen einer Gefährdung. Wichtige Entwicklungen sollten verfolgt und dem Vorstand gemeldet werden. Und natürlich muss ihnen auf technischer Ebene die gebührende Priorität eingeräumt werden.

4. Prioritäten statt Durchschnittswerte

Sich auf das Wesentliche zu konzentrieren bedeutet auch, dass wir mit Durchschnittswerten vorsichtig sein müssen. Durch die Bildung von Durchschnittswerten können Abweichungen von kritischen Kontrollen unter dem Radar bleiben und Ausreißer bleiben unentdeckt. Wir empfehlen daher, die Ergebnisse aller Hunderte von Kontrollen, die Sie identifiziert haben, nicht zu aggregieren. Aus technischer Sicht mag es attraktiv sein, einen prozentualen Abdeckungsgrad für den gesamten Rahmen zu ermitteln, aber diese Mittelwertbildung führt dazu, dass die wichtigsten Probleme verborgen bleiben.

Ebenso kann ein Durchschnittswert innerhalb einer bestimmten Kontrolle wichtige Risiken verbergen. Wenn eine Organisation beispielsweise anstrebt, kritische Schwachstellen innerhalb von drei Tagen, Schwachstellen mit mittlerem Risiko innerhalb eines Monats und alle anderen innerhalb von drei Monaten zu patchen, könnte ein Durchschnittswert für die Patching-Leistung die kritischsten Schwachstellen verbergen.

Berichten Sie Durchschnittswerte nur, wenn es für eine bestimmte KCI sinnvoll ist. Ausführlichere Hinweise zu den KCIs und der Abdeckung finden Sie im Weißbuch Berichterstattung über Cyber-Risiken an Vorstände.

5. Berichtslücken statt "alles im grünen Bereich"

Es ist völlig in Ordnung, dem Verwaltungsrat die tatsächliche Situation zu melden, einschließlich der zu schließenden Lücken. Er muss dies hören, wenn es der Realität entspricht. Dies wird der Organisation auch helfen, die aufsichtsrechtlichen Bestimmungen einzuhalten und die Priorisierung von Investitionen zu untermauern.

Bei der Meldung von Lücken an den Verwaltungsrat muss erläutert werden, welches Risiko sie mit sich bringen und welche Maßnahmen vorgeschlagen werden, um sie in einem voraussichtlichen Zeitrahmen zu beheben.

6. Eingebettet und nicht abgekoppelt

Die Wirkung der Berichterstattung über Cyberrisiken an den Vorstand wird dadurch verstärkt, dass diejenigen, die sie verwalten (Betreiber, Manager), Zugang zum Status der Kontrollen erhalten. Wir nennen dies die "Demokratisierung der Metriken".

Die Berichterstattung über Cyber-Risiken an den Vorstand ist ein wesentlicher Faktor für die Organisation. Was als wichtig gemeldet wird, wird unweigerlich (glücklicherweise) auch vom Vorstand und innerhalb des Unternehmens als

wichtig wahrgenommen. Die gemeldeten KCIs sollten daher aus Sicht des Risikomanagements sinnvoll sein und den wahren Status des Risikos aufzeigen.

Die Daten, die den KCIs zugrunde liegen, sollten von den Systemen gesammelt werden, die die Kontrollen durchführen. Die Implementierung verbundener Metrik-Dashboards auf allen Ebenen der Organisation mit der erforderlichen Granularität, um den Managern der Kontrollen Einblick zu gewähren, schafft Transparenz, erhöht die Eigenverantwortung und ermöglicht die Feinabstimmung des Systems.

7. Transparenz von Abweichungen statt Akzeptanz

Sie können Abweichungen von den Schlüsselkontrollen sichtbar machen, indem Sie sie dem Vorstand melden. Diese Abweichungen können auf die Übernahme von Risiken oder auf (absichtliche oder versehentliche) Verstöße gegen die Richtlinien zurückzuführen sein.

In den meisten Unternehmen gibt es ein Verfahren, das es den Abteilungen erlaubt, von den Sicherheitsrichtlinien abzuweichen, indem sie "das Risiko in Kauf nehmen". Anstatt diese Abweichungen unter dem Radar zu halten, wäre es ratsam, sie zu melden. Die Sichtbarmachung von Abweichungen könnte dem Unternehmen helfen, sich auf die Schlüsselkontrollen auszurichten, die das Risiko mindern und die Risikobereitschaft einhalten sollen.

Die Überwachung von Abweichungen ist besonders nützlich, um den Reifegrad der Organisation in Bezug auf Risikomanagementprozesse und -kultur zu verstehen. Reifere Unternehmen neigen dazu, "Risikoakzeptanz" als letzte der verfügbaren Optionen zu behandeln, nicht als erste.

Die Dokumentation dieser Abweichungen ermöglicht es uns auch, unrealistische Schwellenwerte zu ermitteln, z. B. die Behebung aller Schwachstellen mit einem Budget von 1 % der ARR. Durch die Diskussion der Abweichungen kann die gesamte Organisation zu Risikoakzeptanzschwellen übergehen, die praktischer und realistischer sind.

8. Risikobereitschaft statt Nullrisiko

Wir können es nicht oft genug wiederholen: Ein Unternehmen muss auf Vorstandsebene festlegen, was ein akzeptables Maß an Cyberrisiken ist. Ein Nullrisiko ist ein unmögliches und wahrscheinlich sogar unerwünschtes Ziel. Es geht im Wesentlichen um Risikovermeidung und nicht um einen "effizienten Umgang mit dem Risiko". In vielen Unternehmen ist diese Risikobereitschaft bereits im Rahmen der allgemeinen Geschäftsrisikoprozesse festgelegt worden.

Wenn dies für den Cyberbereich noch nicht der Fall ist, sollte der CISO den Vorstand auffordern, die Risikobereitschaft für den Cyberbereich zu bestimmen:

- Wie viel sind wir bereit zu verlieren, wenn sich das Cyber-Risiko verwirklicht? Denken Sie an tagelange Ausfallzeiten, Diebstahl von Rechten des geistigen Eigentums, Verlust von personenbezogenen Daten, Rufschädigung...
- In welchem Umfang soll das Risiko gemindert werden? Ein Nullrisiko ist ein unmögliches Ziel. Angesichts der Entwicklung der

Bedrohungslandschaft und der verfügbaren Technologie dürfte die Risikobereitschaft für Cyberrisiken zwischen hoch und mittel schwanken.
- Welche Ressourcen/Budgets sind wir bereit, für Abhilfemaßnahmen zur Verfügung zu stellen?
- Wollen wir das verbleibende Cyber-Risiko versichern oder selbst versichern?

Ein quantitativer Ansatz für die Risikobereitschaft in Bezug auf Cyberrisiken ist derzeit schwer zu verwirklichen und eher die Ausnahme als die Regel. Die Erklärung zur Risikobereitschaft (Risk Appetite Statement - RAS) basiert in der Regel auf einem qualitativen Ansatz, der qualitative und quantitative Elemente kombiniert. Das RAS-Niveau wird vom Vorstand in Form von niedrig, mittel und hoch festgelegt. Oft wird sie durch den Vergleich verschiedener Risikobereiche und deren Priorisierung festgelegt. Es handelt sich hierbei vielmehr um eine Kalibrierung der verschiedenen Bereiche. Die eigentliche Untermauerung des RAS ist eine echte Herausforderung. Sie erfordert eine Vielzahl von Indikatoren, die von der technischen/operativen Ebene bis zur Management- und Strategieebene reichen.

Die Ermittlung/Definition von Cyber-Risiken in Bezug auf die monetären Auswirkungen des Geschäfts ist sinnvoll. Das Ziel dabei ist nicht Perfektion. Die initialen Annahmen zu Zahlen können falsch sein. Bringen sie die Führungskräfte darauf, diese Fragen auf wiederholbare Weise zu beantworten. Sie sollten Cyber-Risikos als Geschäftsrisiko wahrnehmen und diese auf ähnliche Weise angehen.

9. Die Geschichte erzählen - Risikoverbindung zu Dienstleistungen

Ein CISO muss die Cyber-Geschichte in einem geschäftlichen Kontext erzählen, damit die Botschaft ankommt. Dazu muss er den Status der Kontrollen und ihre Auswirkungen auf das Risikoprofil verstehen, das durch die Geschäftsdienste bestimmt wird.

Ein wichtiges Ziel für Organisationen, die einen hohen Reifegrad ihres Risiko- und Kontrollumfelds anstreben, ist die Fähigkeit zu verstehen:

- wie sich ihre Geschäftsdienstleistungen (z. B. Kreditvergabe oder Handel) auf das mit dem Cyberspace verbundene Risikoprofil auswirken (z. B. die Notwendigkeit, vertrauliche Kundendaten sicher zu speichern)
- und umgekehrt: wie sich das inhärente Cyber-Risiko auf diese Dienste auswirken kann (z. B. kann das Fehlen einer sicheren Speicherung von eingeschränkten Kundendaten zu einer versehentlichen Offenlegung von Daten führen oder den Datenzugriff für böswillige Akteure erheblich erleichtern).

Die Organisation muss sicherstellen, dass sie versteht, welche IT-Assets und -Prozesse ihre Geschäftsprozessse unterstützen (z. B. welche Systeme für die Bereitstellung eines Kredits erforderlich sind). Dies ermöglicht die Erstellung eines Profils und die Messung des inhärenten Cyber-Risikos.

Der nächste Schritt besteht darin, sicherzustellen, dass Cyber-Kontrollen auf die IT-Ressourcen und -Prozesse mit automatisierten Methoden (z. B. "Kontrollen als

Code") angewandt und implementiert werden, so dass die Wirksamkeit anhand von Schlüsselkontrollindikatoren (z.B. KCI5 „% richtlinienkonform konfigurierte Endpunkte“) eindeutig gemessen werden kann.

Dieser Ansatz ermöglicht es dem CISO, dem Vorstand eine klare Aussage darüber zu machen, wie sich der aktuelle Restrisikostatus und bekannte Kontrollmängel auf das Unternehmen auswirken können, und den Kontext zu liefern, um die Risikobereitschaft erfolgreich zu verwalten und relevante Investitionsentscheidungen zu treffen.

10. Vereinheitlichung der Cyber-Vorschriften - selektive Anwendung des "Gold-Plating" '

Die meisten aktuellen und neu entstehenden Cyber-Vorschriften auf der ganzen Welt haben sich überschneidende Anforderungen. Ein CISO sollte alle für seine Organisation relevanten Vorschriften an den verschiedenen geografischen Standorten und in den verschiedenen Sektoren umsetzen, indem er Zuordnungen verwendet, um ihre Umsetzung zu vereinheitlichen.

Dieser Ansatz ermöglicht die Anwendung der gleichen Logik und des gleichen Grundprinzips bei der Behandlung ähnlicher Risiken und Kontrollen, unabhängig von der jeweiligen Verordnung, mit einer erheblichen Reduzierung des Aufwands für den CISO und die technischen Teams.

Allerdings gibt es immer wieder Ausnahmen. Einige Vorschriften können spezifische Kontrollen vorschreiben, die nur für eine bestimmte Einrichtung gelten und deren Einhaltung möglicherweise schwierig ist. In solchen Fällen kann man sich für eine "Gold-Plating"-Strategie entscheiden, bei der diese Kontrollen ausschließlich für diese Einheit isoliert werden. Diese selektive Anwendung minimiert die überflüssige Arbeit für andere Stellen innerhalb der Organisation und ermöglicht die Aufrechterhaltung einer umfassenden Cybersicherheitsstrategie und eines umfassenden Berichts.

Die Berichtslinie(n) des CISO

Ein CISO hat die Aufgabe, die Vision, die Strategie und das Programm der Organisation zum Schutz von Informationen und technologischen Werten festzulegen und aufrechtzuerhalten. Der CISO sollte in der Lage sein, selbständig und unabhängig zu handeln (z. B. DORA Art. 6.4[6]). Traditionell ist der CISO einer Führungskraft aus der C-Suite unterstellt, beispielsweise dem Chief Information Officer (CIO), Chief Operating Officer (COO), Chief Finance Officer (CFO) oder sogar dem CEO. Diese Struktur ist zwar weit verbreitet, aber die CISOs können sich in einer widersprüchlichen Position befinden, wenn der betreffende C-Suite Executive auch für andere Funktionen verantwortlich ist, die Entscheidungen über Kompromisse zwischen der Einhaltung von Sicherheitsstandards und der betrieblichen Effizienz usw. erfordern.

Um zu vermeiden, dass der CISO isoliert handelt, müssen wir ein Gleichgewicht zwischen den Interessen der internen Stakeholder und der Minderung des Cyberrisikos wahren. Eine Organisation kann einen Lenkungsausschuss für

[6] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554 (Artikel 6)

Informationssicherheit (SteerCo) einrichten, der den Auftrag hat, operative Entscheidungen zu treffen, Sicherheitsrisiken und Schlüsselkontrollen zu überwachen, Messgrößen zu vereinbaren, Budgets zu genehmigen, die Sicherheitsstrategie zu validieren und ihre wirksame Umsetzung zu überwachen.

Die Effektivität des SteerCo hängt von der Teilnahme relevanter C-Suite-Mitglieder ab, wie dem Chief Risk Officer (CRO), Chief Operating Officer (COO), Chief Compliance Officer (CCO), Chief Information Officer (CIO), Chief Financial Officer (CFO), Legal Counsel und natürlich dem CISO. Ein weniger häufiges, aber mit Befugnissen ausgestattetes SteerCo ist häufigen SteerCo-Sitzungen mit begrenzter Entscheidungsbefugnis vorzuziehen.

Die Berichterstattung über Cyber-Risiken an den Vorstand würde in den Aufgabenbereich des CISO fallen, idealerweise in Absprache oder zumindest in voller Transparenz mit dem SteerCo. Der CISO sollte über eine unabhängige Berichtslinie zum Vorstand oder einem seiner Unterausschüsse, wie dem Prüfungsausschuss, verfügen. Die Häufigkeit der Berichterstattung über Cyber-Risiken an den Vorstand sollte der Wesentlichkeit des Risikos für das Unternehmen entsprechen, aber ein vierteljährlicher Bericht wäre eine gute Praxis, wenn er mit einem Eskalationsprozess für den Bedarfsfall kombiniert wird.

Dieses Modell kombiniert eine effektive Entscheidungsbefugnis mit einer soliden und wirksamen Governance.

Produkt-, Portfolio- und Lieferketten-Cyberrisiken

Die in unseren Whitepapers beschriebenen Grundsätze für die Berichterstattung über Cyber-Risiken in Unternehmen an die Vorstände lassen sich leicht auf *Cyber-Risiken bei Produkten* (wie gut sind Ihre Produkte geschützt?), *Cyber-Risiken bei Portfolios* (welche Schlüsselkontrollen möchten Sie Ihren Portfolio-Unternehmen auferlegen und wie möchten Sie die Einhaltung dieser Schlüsselkontrollen messen?) sowie *Risiken in der Lieferkette* (Schlüsselwerte, Abhängigkeit, Schlüsselkontrollen und wie die Einhaltung gemessen und berichtet werden soll) übertragen und erweitern. Die KCIs können sich in diesen Bereichen unterscheiden, aber dennoch ähnliche Grundsätze anwenden.

Vergleiche mit Gleichartigen

In einer branchenübergreifenden Gemeinschaft von vierzig Unternehmen, die sich über einen Zeitraum von zwei Jahren vierteljährlich in einer CISO-Arbeitsgruppe zusammenfanden, konnten wir eine weitgehende Übereinstimmung mit den in diesem White Paper dargelegten Grundsätzen feststellen.

Wir hoffen, dass der Austausch dieser Praktiken innerhalb der breiteren Gemeinschaft den Weg für den Vergleich von Notizen (und Ergebnissen) mit Gleichgesinnten innerhalb des Sektors und sogar für die Anwendung dieser Grundsätze bei der Interaktion mit den Regulierungsbehörden ebnen wird.