Berichterstattung über Cyber-Risiken an Vorstände

CISO-Ausgabe

Kontrolle, Messung, Bericht, Wiederholung

Autoren
Freddy Dezeure
George Webster
Jason Trost
Eireann Leverett
João Pedro Gonçalves
Patrick Mana
Greg McCord
Josh Magri

Rezensenten
Lokke Moerel
Alex Iftimie
Chris Deverell
Greg Bell
Jamie Hutchinson

Datum: 14. März 2022
Version: Endgültige Fassung

Inhaltsverzeichnis

Einführung

Dieses Dokument bietet Methoden und Anregungen für Chief Information Security Officers (CISO), um quantitative Metriken für die Cybersicherheit zu entwerfen und zu implementieren, um auf Vorstandsebene über Cyberrisiken zu berichten und hinreichende Sicherheit zu bieten, dass das Risiko innerhalb der akzeptierten Risikobereitschaft liegt.

Früher konnten Sie Ihre Geheimnisse schützen, indem Sie einen Schlüssel in einer geschlossenen Tür umdrehten. Für Ihre tiefsten Geheimnisse haben Sie vielleicht eine bessere Tür eingebaut, vielleicht die Wände verbessert oder ein paar Wachen aufgestellt. Wenn Sie Ihre Geheimnisse transportieren mussten, haben Sie sie in eine Tasche gepackt und Steganografie oder Kryptografie verwendeten, um das Geheimnis vor neugierigen Blicken zu schützen. Dieses Märchen galt auch für Computer, aber diese Zeit ist längst vorbei. Unsere Gesellschaft, unsere Wirtschaft und unser tägliches Leben hängen vom Austausch von Informationen ab, die durch unsere vernetzten Systeme fließen. Das Konzept eines schützenden Zauns gehört der Vergangenheit an.

Die moderne Wirtschaft und ihre Abhängigkeit von Daten haben dazu geführt, dass unsere Geheimnisse immer wertvoller werden, was die Aufmerksamkeit von Berufsverbrechern auf sich gezogen hat, die unsere Abwehrmechanismen immer stärker auf den Zahn fühlen. Unsere Informationssysteme stellen für Regierungen, Unternehmen und Privatpersonen gleichermaßen ein erhebliches Risiko dar. Im Jahr 2021 beliefen sich die durchschnittlichen Kosten für eine Datenpanne bei einem typischen Unternehmen auf 4 Millionen Dollar. Eine größere Sicherheitsverletzung kann Kosten von über 400 Millionen Dollar verursachen[1] . Die Gesamtkosten für alle Cybersicherheitsvorfälle im Jahr 2020 werden auf 1 Bio. $ geschätzt, was einem Anstieg von mehr als 50 % innerhalb von zwei Jahren entspricht[2].

Es ist nicht verwunderlich, dass das Thema Cybersicherheit für die meisten Organisationen und Regierungen zu Recht ganz oben auf der Tagesordnung steht. So enthalten beispielsweise die neuen SEC-Vorschriften über die Offenlegung von Cybersicherheitsrisiken Bestimmungen über die Bedeutung der Kommunikation von Cybersicherheitsrisiken an Vorstände[3].

Die Aufmerksamkeit führender Interessengruppen alleine löst weder die Probleme der Cybersicherheit noch verringert es das Risiko. Unsere Führungskräfte in Unternehmen und Behörden sind für den Umgang mit der Cybersicherheit schlecht gerüstet, weil sie deren Sprache nicht sprechen. Umgekehrt ist die Cybersicherheit schlecht für den Umgang mit hochrangigen Interessenvertretern geeignet, da es für Cyberexperten schwierig ist, die Effektivität ihres Programms zu messen, den Nutzen des Programms zu formulieren oder gar seine Erfolge zu kommunizieren. Diese Unfähigkeit, die Effektivität von Cybersicherheitskontrollen zu messen und die Risikominderung, die sie bewirken, den leitenden Interessenvertretern mitzuteilen, bringt Fachleute für Cybersicherheit in eine Position, in der sie um das Budget

[1] https://www.ibm.com/security/data-breach
[2] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
[3] https://www.mofo.com/resources/insights/220311-sec-proposes-cybersecurity-disclosure-rules.html

kämpfen, ohne zu wissen, ob das, was sie tun, tatsächlich das Verlustrisiko reduziert.

Ein Nullrisiko ist unerreichbar und unrealistisch. Das war schon immer so. Aber die Dynamik hat sich verändert. Darüber hinaus übersteigt die Geschwindigkeit, mit der sich die Bedrohungslandschaft im Bereich der Cybersicherheit verändert, unsere Fähigkeit, Kontrollen an das Risiko anzupassen oder auch nur festzustellen, welche Kontrollen für die Risikominderung wichtig sind. Ein CISO muss das Cybersicherheitsbudget rechtfertigen und erklären, warum die ausgewählten Ansätze mit der allgemeinen Risikobereitschaft des Unternehmens übereinstimmen. Dies ist eine anspruchsvolle Aufgabe, für die dieses Dokument jedoch Anregungen und Material für die Entwicklung und Umsetzung pragmatischer Lösungen liefern soll.

Zweck

Dieses Papier enthält Anhaltspunkte für CISOs, wie sie ihren leitenden Interessenvertretern, z. B. ihrem Vorstand, über Cyberrisiken und deren Kontext berichten können. Es beschreibt Methoden, die CISOs dabei helfen, wie sie das Thema Cyber-Risikomanagement angehen, dies effektiv kommunizieren und eine angemessene Aufsicht ermöglichen. Obwohl der Inhalt dieses Dokuments nicht im Mittelpunkt steht, hilft es auch bei der Berichterstattung über Cyberrisiken an andere Interessengruppen wie Aufsichtsbehörden, Versicherer und Kunden.

Wir sind der Meinung, dass Messgrößen ein notwendiger Bestandteil jeder erfolgreichen Arbeit sind. Die Managementtheorien von Peter Drucker sind ein Beweis dafür und haben die Wirtschaft verändert. Bei der Cybersicherheit ist das nicht anders. Metriken werden benötigt, um das Risikomanagement in Unternehmen zu steuern, die Widerstandsfähigkeit gegenüber Cyberangriffen im Laufe der Zeit zu erhöhen und die Einhaltung der Vorschriften gegenüber internen und externen Interessengruppen nachzuweisen. Allerdings muss man die richtigen Dinge messen und das Problem ganzheitlich betrachten. Leider ähnelt die Messung von Cybersicherheitsrisiken und die Anwendung einer geeigneten Metrik der Suche nach dem heiligen Gral. Es gibt nur wenige bewährte Verfahren für Metriken, ihre Verbreitung in der Community ist selten, und die Risikomessung in einer nicht deterministischen Bedrohungslandschaft für die Cybersicherheit ist eine Herausforderung.

Dieses Papier fasst die Ergebnisse und bewährten Verfahren einer CISO-Arbeitsgruppe zusammen. Den Teilnehmern gebührt volle Anerkennung. Ohne ihre Erkenntnisse, ihren Austausch und ihre Interaktion wäre dieses Papier nicht zustande gekommen. Das Papier enthält Anhänge mit Beispielen aus der Community. Wir hoffen, weitere Beiträge zu erhalten, so dass ein neuer Bestand an Arbeiten und Beispiele für Implementierungen entstehen. Um die Interaktion und den Austausch in der Community zu fördern, planen wir für die Zukunft weitere Veröffentlichungen.

Erwartungen des Vorstands

In der Regel legen Vorstände Wert auf:

- Strategische Positionierung und Wachstum des Unternehmens
- Shareholder Value, Markenschutz
- Strategische Pläne, Ressourcenzuweisung, Managementvergütung
- Überwachung der Einhaltung von Vorschriften (staatliche und sektorale Vorschriften, ESG)
- Kritische Geschäftsrisiken - einschließlich Cybersicherheit
- Vergleich mit Sektor/Peers
- Die treuhänderische Haftung der einzelnen Vorstandsmitglieder.

Für die meisten dieser Bereiche gibt es eine etablierte Praxis, wie man Nachweise in einer Art und Weise erhebt und berichtet, die hilfreich ist und einen angemessenen Grad an Granularität und Verteilung der Verantwortung/Delegation besitzt.

Was die Cybersicherheit betrifft, so ist die gängige Praxis in der Branche weniger ausgereift. Häufig fühlen sich Vorstände nicht ausreichend kompetent, um Cyberrisiken zu verstehen, oder sie halten Cyberrisiken für zu technisch, genehmigen Ressourcen und delegieren dieses Risiko.

Vorstände erkennen oft nicht die kontinuierliche Bedeutung der Cybersicherheit und reagieren reflexartig auf aktuelle Meldungen in den Medien, um sie dann schnell wieder zu vergessen, bis der nächste große Cybervorfall eintritt. In der Regel wird Cybersicherheit erst dann zu einem Thema, wenn es bereits zu spät ist.

Dies wird mitunter durch eine undurchsichtige Managementkultur unterstrichen, die systematisch „alles im grünen Bereich" melden, während die meisten Vorstände in Wirklichkeit gerne mehr über Lücken und darüber erfahren würden, wie diese Lücken behoben werden können.

In Fällen, wo Vorständen über Cybersicherheit berichtet wird, gibt es eine Vielzahl von Methoden, Werkzeugen und Prozessen, die eingesetzt werden. Die Unternehmen wissen nicht, was sie berichten sollen und wie sie ein wirksames Feedback vom Vorstand erhalten.

Risiko als entscheidender Faktor

In unserem Cyber-Umfeld müssen wir Entscheidungen darüber treffen, was wir wie schützen wollen. Perfekte Sicherheit ist eine Illusion und die Ressourcen sind knapp. Bewertungen und Entscheidungen über Prioritäten werden durch die Anwendung der bewährten Verfahren der Risikobewertung erleichtert und objektiviert.

Es gibt verschiedene Definitionen von Risiko, die sich auf die Möglichkeit eines unerwünschten Ergebnisses infolge eines Vorfalls, Ereignisses oder Vorgangs konzentrieren, das durch seine **Wahrscheinlichkeit** und die damit verbundenen **Auswirkungen** bestimmt wird[4]. Ein reales Beispiel für ein Risiko ist die Möglichkeit, infolge einer Pandemie zu sterben oder schwer zu erkranken.

[4] https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf

Für unsere Diskussion werden wir das erweiterte Modell verwenden, bei dem sich das Risiko aus den drei Faktoren **Bedrohung** x **Schwachstelle** x **Auswirkungen** zusammensetzt. In dieser Gleichung wird die Wahrscheinlichkeit zu einer Kombination aus Bedrohung und Anfälligkeit erweitert, was im Kontext der Cybersicherheit hilfreich ist. Wir behandeln keine versehentlichen Vorfälle.

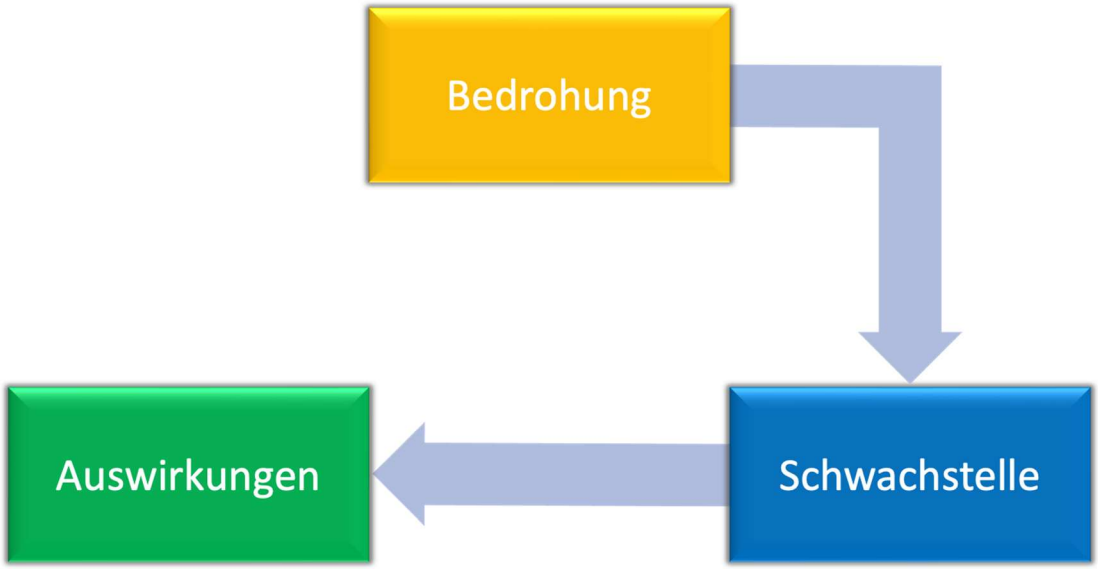


Abbildung 1 Risiko als Kombination aus Bedrohung, Schwachstelle und Auswirkungen

Die Bedrohung liegt meist außerhalb unserer Organisation und ist eng mit den Gegnern verbunden. Die Identifizierung unserer Hauptgegner und ihrer Motive ist wichtig für die Festlegung von Prioritäten. Wir können aktuelle Bedrohungen beobachten und versuchen, zukünftige Bedrohungen vorherzusagen. Spezialisierte Nachrichtendienste und Regierungsstellen können uns dabei helfen, zu verstehen, welche Gegner wir haben, welche Motive sie haben, welche Mittel und Methoden sie einsetzen und wie sie vorgehen, um ihre Ziele zu verfolgen.

Der zweite Faktor ist die **Schwachstelle**, auf die wir durch die Entwicklung und Umsetzung von Kontrollen am meisten Einfluss nehmen können. Die Identifizierung von Schlüsselkontrollen, die Berücksichtigung unserer wichtigsten Vermögenswerte und die Motivation und Methoden unserer wichtigsten Gegner sind wichtig für die Festlegung von Prioritäten.

Die **Auswirkungen** betreffen den Diebstahl von geistigem Eigentum, den Verlust personenbezogener Daten, die Unterbrechung von Diensten, die Schädigung von Personen und die Schädigung von Marken. Die Auswirkungen sind eng mit den Vermögenswerten verbunden. Die Identifizierung unserer wichtigsten Vermögenswerte ist wichtig für die Festlegung von Prioritäten.

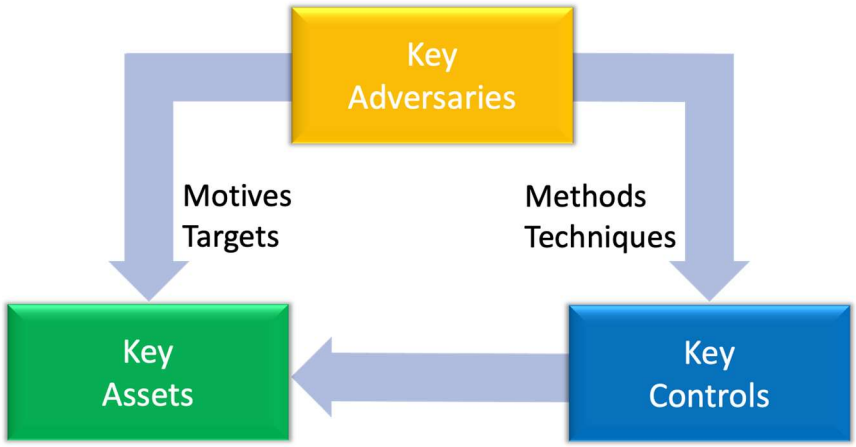


Abbildung 2 Cyber-Risiko durch Angreifer, die Schwachstellen ausnutzen

Wir sind der Meinung, dass wir das Problem der Cybersicherheit als ein Problem des Risikomanagements angehen und ein fundiertes Risikomanagement und eine Risikominderung einsetzen sollten, um die Maßnahmen kontinuierlich zu priorisieren. Cyber muss in das gesamte Managementsystem integriert werden. Es sollte nicht als etwas Besonderes/Isoliertes betrachtet werden, sondern als integraler Bestandteil der organisatorischen Aktivitäten und Prozesse, einschließlich des Risikomanagementprozesses. Dies erfordert eine Anpassung der Methoden und des Vokabulars.

Zur Veranschaulichung der relevanten Informationsflüsse im vorliegenden Dokument wird das Diagramm in Abbildung 3 verwendet, das sich am NIST Cyber Security Framework[5] orientiert.

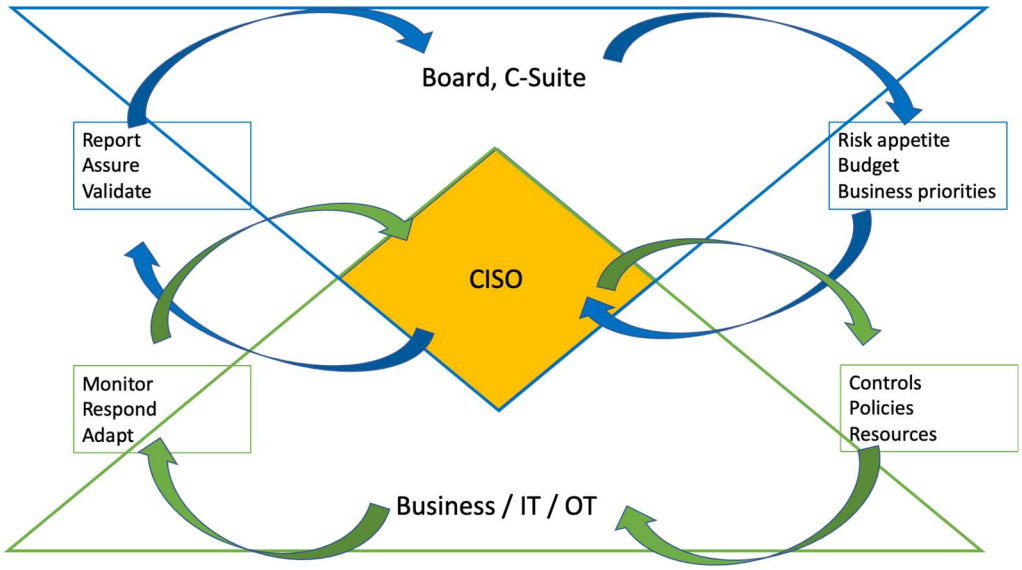


Abbildung 3 Informations- und Entscheidungsflüsse. Inspiriert durch NIST CSF

Wir können einen oberen, leitenden Teil und einen unteren, implementierenden/operativen Teil unterscheiden, mit dem CISO in der zentralen Überschneidungszone, die die operative Ebene der Cybersicherheit mit der strategischen Ebene verbindet.

[5] https://www.nist.gov/cyberframework

Treffen wichtiger Entscheidung

Unternehmen müssen grundlegende Entscheidungen für das Cyber-Risikomanagement treffen. Diese werden auf der rechten Seite des Diagramms veranschaulicht: welche sind die wichtigsten Vermögenswerte, wie hoch ist die Risikobereitschaft und welche sind die wichtigsten Kontrollen/Maßnahmen, die eingeführt werden müssen. Damit verbunden sind auch das Budget und die Ressourcenzuweisung für Maßnahmen und Personal im Bereich Cybersicherheit.

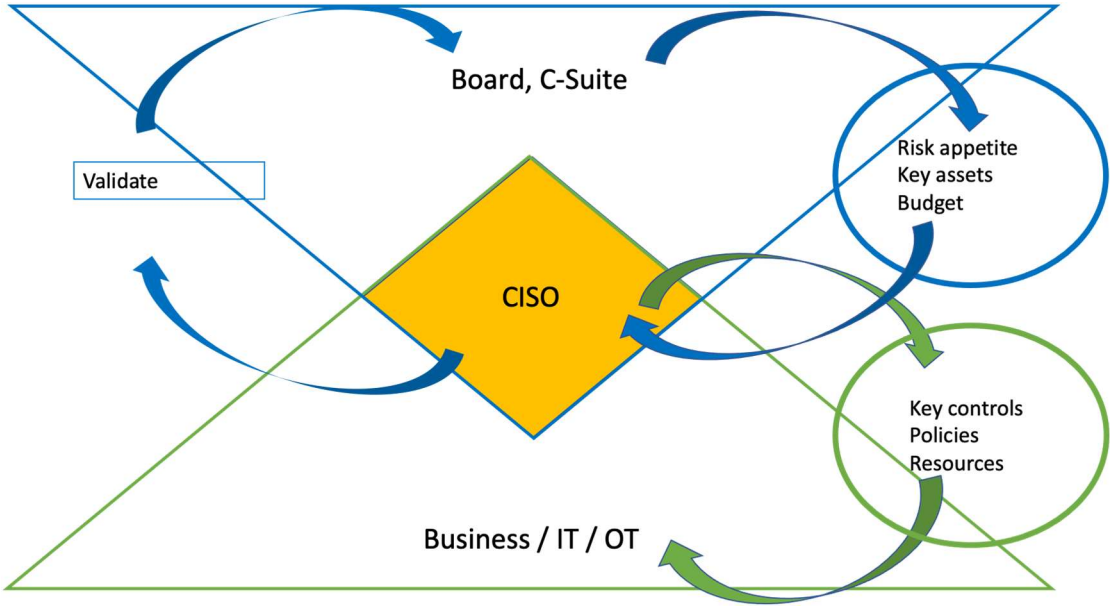


Abbildung 4 Zu treffende Entscheidungen

Es ist von entscheidender Bedeutung, dass diese vom CISO vorgeschlagenen Entscheidungen in der gesamten Organisation (Cybersicherheit, Risiko, IT/OT, operativer Bereich) vereinbart und abgestimmt sowie auf Führungsebene verstanden/genehmigt und auf dem neuesten Stand gehalten werden.

Wichtige Vermögenswerte – Kronjuwelen

In den meisten Unternehmen ist es unerschwinglich, alle Vermögenswerte gegen alle möglichen Cyberbedrohungen zu schützen. Es müssen Prioritäten festgelegt und Ressourcen für die wichtigsten Bedrohungen der wichtigsten Vermögenswerte bereitgestellt werden. Die Identifizierung dieser zentralen Vermögenswerte ist ein wesentlicher Bestandteil des Risikomanagements im Allgemeinen und des Risikomanagements im Bereich der Cybersicherheit im Besonderen.

Es ist keine einfache Aufgabe, die eine funktionsübergreifende Analyse und Bewertung erfordert, wobei die potenziellen Auswirkungen auf die Geschäftskontinuität, den Datenschutz, die Regulierung und die langfristige Wettbewerbsposition (geistiges Eigentum) zu berücksichtigen sind.

Bei der Ermittlung (und Aktualisierung) der Liste der wichtigsten Vermögenswerte sollte ein CISO nicht nur die IT-Vermögenswerte (Rechenzentren, Sicherungssysteme, Active Directory usw.), sondern auch die relevanten Informationswerte (Repositorys, geistiges Eigentum), die

Geschäftswerte (Buchhaltung, Produktionsmanagement, Logistik, physischer Zugang) usw. berücksichtigen.

Es wird viel von der Identifizierung der wichtigsten Vermögenswerte oder "Kronjuwelen" gesprochen, was wiederum eine probabilistische Risikobewertung und damit ein Ausdruck der Überzeugung ist, dass ein Angreifer mit größerer Wahrscheinlichkeit x als y stehlen wird. Ein weiteres Schlüsselelement der probabilistischen Argumentation ist jedoch die Aktualisierung dieser Annahmen auf der Grundlage aktueller Cyber-Bedrohungen. Cryptojacking zum Beispiel interessiert sich nicht für Ihre Kronjuwelen und begnügt sich damit, weniger wichtige Werte anzugreifen.

Es ist wichtig, die Wahrscheinlichkeit verschiedener Cyber-Bedrohungen (DDoS, Ransomware, gezielter IP-Diebstahl, opportunistische Angriffe, Phishing, Betrug, Malware-Infektion – diese Liste lässt sich beliebig fortsetzen) in Bezug auf die Erörterung der wichtigsten Vermögenswerte zu bewerten – des einen Müll ist des anderen Schatz.

Risikobereitschaft

Um Maßnahmen zur Risikominderung und -kontrolle zu ermitteln, muss ein Unternehmen auf Führungsebene festlegen, welches Maß an Kontrolle „ausreichend" ist und was ein akzeptables Risikoniveau darstellt.

Dabei sollten wir die Risikobereitschaft in einer quantifizierbaren Weise ausdrücken, indem wir einen Schwellenwert oder eine grafische Darstellung von akzeptablen und nicht akzeptablen Situationen verwenden. Manche Unternehmen verwenden monetäre Schwellenwerte für die Risikobereitschaft, während andere (Verkehrsgewerbe, Krankenhäuser usw.) den Schwellenwert auf das Risiko von Verletzungen oder den Verlust von Menschenleben beziehen. In einigen Fällen kann sich die Risikobereitschaft auf die Geschäftskontinuität oder die akzeptable Dauer der Unterbrechung von Dienstleistungen beziehen.

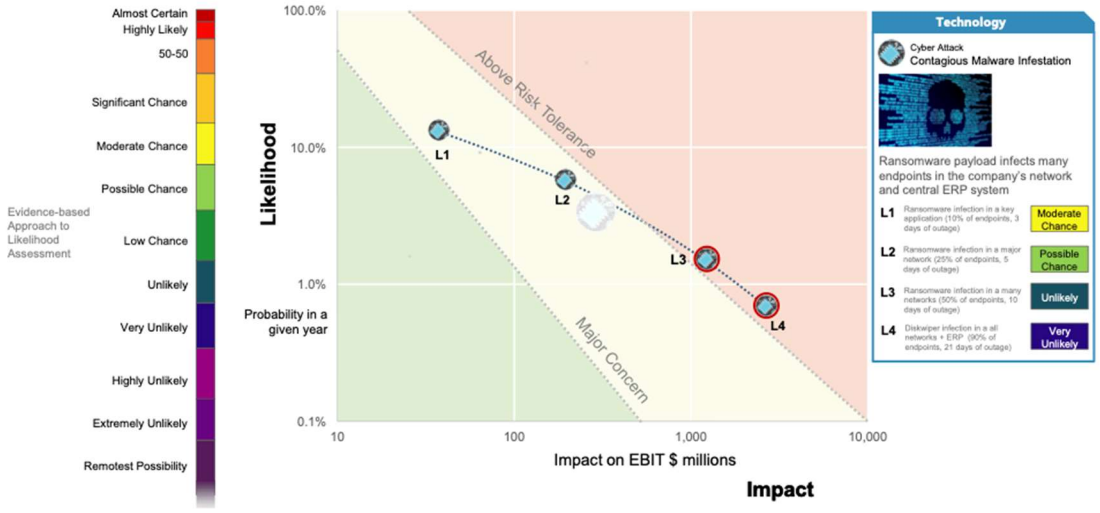


Abbildung 5 Beispiel für die Zuordnung zum Risiko, Quelle: Zentrum für Risikostudien, Universität von Cambridge

Rahmenwerk(e) für Cybersicherheit und Schlüsselkontrollen

Rahmenwerke für Cybersicherheit sind ein Instrument zum kohärenten Umgang mit Cybersicherheitsrisiken und zur Umsetzung einer Cybersicherheitsstrategie für Unternehmen. Weit verbreitete Kontrollrahmen sind ISO/IEC 27001[6], das Cyber Security Framework (CSF) von NIST[7], das davon abgeleitete CRI Profile[8], NIST SP 800-53[9] sowie die CIS Critical Security Controls[10]. Alternativ oder in Kombination dazu verwenden viele Unternehmen auch das bedrohungsorientierte MITRE ATT&CK® Framework[11]. Auch wenn viele Gründe für die Wahl eines einzigen Rahmenwerks sprechen könnten, haben alle ihre Besonderheiten. Es ist nicht so wichtig, welches Rahmenwerk ausgewählt wird, da es Entsprechungen zwischen ihnen gibt. Es ist jedoch wichtig, sich für ein System zu entscheiden und dieses beizubehalten, damit die Organisation ihre Fortschritte im Laufe der Zeit messen kann.

Es ist sehr ratsam für jede Organisation, sich intern auf das Rahmenprofil zu einigen, das sie für ihre Cybersicherheitsstrategie und Risikominderung verwenden will. Ohne eine solche interne Abstimmung zwischen CISO, IT/OT und Risikomanagement ist es schwierig, den Vorstand für Cyberfragen zu gewinnen.

Ein guter Ausgangspunkt für die Ermittlung und Überwachung von Schlüsselkontrollen ist die Darstellung der Einhaltung der grundlegenden Cybersicherheitsleitlinien der nationalen Cybersicherheitsbehörden. Wir haben eine Auswahl relevanter Quellen in Anhang 1 aufgenommen. Es gibt ein hohes Maß an Überschneidungen zwischen diesen verschiedenen grundlegenden Leitlinien, die noch auf die spezifische Situation einer Organisation übertragen werden müssen. Sie bieten jedoch einen hervorragenden, prägnanten und praktischen Ausgangspunkt.

Einige wichtige Kontrollen, die immer enthalten sind:

- K1: Führen eines aktuellen Verzeichnisses aller (wichtigen) Vermögenswerte und Abhängigkeiten;
- K2: Erstellen zuverlässiger, gültiger, sicherer und geschützter Backups der wichtigsten Daten;
- K3: Erzwingen einer mehrstufigen Authentifizierung(soweit möglich)
- K4: Beschränken der Zugriffsberechtigungen der Benutzer auf das unbedingt Notwendige;
- K5: Erkennen und rechtzeitiges Beheben wichtiger Sicherheitslücken;
- K6 Sammeln und Analysieren von Protokollen aller (wichtigen) Anlagen;
- K7: Segmentieren des Netzes zum Schutz wichtiger Vermögenswerte;
- K8: Sichern internetfähiger Systeme;
- K9: Einführen eines Verfahrens zur Reaktion auf Vorfälle und zur Wiederherstellung;
- K10: Sensibilisierung der Nutzer (einschließlich der Vorstandsmitglieder).

[6] https://www.iso.org/isoiec-27001-information-security.html
[7] https://www.nist.gov/cyberframework
[8] https://cyberriskinstitute.org/
[9] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[10] https://www.cisecurity.org/controls/cis-controls-list/
[11] https://attack.mitre.org/

In den folgenden Beispielen für Metriken wird auf diese Kennungen der Schlüsselkontrollen Bezug genommen.

Quantitative Metriken

Es ist sinnvoll, die Auswahl eines Rahmenprofils mit der Definition von quantitativen Messgrößen (KPIs, KRIs, KCIs, OKR[12]) mit Zielen/Ergebnissen zu kombinieren und diese mit den relevanten Prozessen/Systemen und Prozessverantwortlichen zu verknüpfen. Diese Metriken können im Laufe der Zeit an den akzeptierten Zielen gemessen und unternehmensweit sowie mit anderen Unternehmen verglichen werden. Einige bewährte Branchenpraktiken zeigen das Potenzial dieses Ansatzes:

- CIS-Kontrollen, Maßnahmen und Metriken[13];
- EPRI Cybersicherheitsmetriken für den Energiesektor[14];
- Die Bibliothek des niederländischen Zahlungsverkehrsverbands für Metriken zur Cyber-Resilienz[15];
- Die KPIs des deutschen Automobilsektors in Verbindung mit ISO[16];
- NIST's Leitfaden zur Leistungsmessung[17].

Die meisten Rahmenwerke gehen davon aus, dass die Organisationen, die sie anwenden, eine Selbstbewertung durchführen, möglicherweise in Kombination mit einer externen Überprüfung durch eine Zertifizierungs- oder Prüfungsstelle. Zu den üblichen Praktiken im Risikomanagement von Unternehmen zählt auch die Selbstbewertung.

Die Überwachung durch Selbstbewertung hat grundlegende Nachteile, wenn es darum geht, den Status der Maßnahmen zur Minderung von Cyberrisiken und deren Wirksamkeit zu ermitteln. Dazu gehören:

- Sie ist subjektiv (keine Aufgabentrennung, gleicher Wissensstand);
- Sie ist nicht ausreichend detailliert;
- Sie ist zeitaufwendig;
- Sie ist zeitlich von den Ereignissen abgekoppelt;
- Es kann nicht zur Alarmierung/Eskalation/Reaktion verwendet werden;
- Zur Abnahme durch Aufsichtsbehörden kann eine unabhängige Prüfung erforderlich sein;
- Sie kann sich auf Indikatoren zum Zeitpunkt der Einführung beschränken (was wurde eingeführt?).

Maschinell erzeugte Daten können eine sehr nützliche Ergänzung zur Selbstbewertung darstellen oder diese sogar weitgehend ersetzen. Sie können die Berichterstattung über Cybersicherheitsrisiken objektiv und wiederholbar machen und automatisieren. Die Identifizierung der maschinell erzeugten Datenquellen und Analysen, die für die Messgrößen benötigt werden, ist ein

[12] Ziele und Schlüsselergebnisse, High Output Management, Andrew S. Grove.
[13] https://www.cisecurity.org/insights/white-papers/cis-controls-v7-measures-metrics
[14] https://www.epri.com/research/products/000000003002010426
[15] https://www.betaalvereniging.nl/wp-content/uploads/Library-of-Cyber-Resilience-Metrics-Shared-Research-Program-Cybersecurity.pdf
[16] https://www.vda.de/vda/en/News/publikationen/publication/vda-isa-catalogue-version-5.0.4
[17] https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft

wichtiger Schritt bei der Entwicklung und Umsetzung eines kohärenten, umfassenden und effektiven Satzes von Metriken.

Die größte Gefahr bei Kennzahlen für Cyberrisiken besteht darin, dass sie die geleistete Arbeit oder den Aufwand widerspiegeln und nicht die Risikominderung. Ein Vorstand oder ein Führungsteam muss sich rigoros gegen die Einbeziehung solcher Metriken wehren. Das ist eine betriebliche Angelegenheit, keine Risikoangelegenheit. Mit anderen Worten: Vermeiden Sie Metriken für die Anzahl der bearbeiteten Vorfälle oder der unter Quarantäne gestellten Malware. Das sind fantastische operative Kennzahlen, aber sie sagen dem Vorstand nicht, ob das Geld, das für die Risikominderung ausgegeben wurde, effektiv eingesetzt wurde. Ein einfaches Hilfsmittel ist, die Risikokennzahl in Form eines Anteils oder eines Verhältnisses anzugeben, wie z. B. Unfälle pro 1000 gefahrene Kilometer. Wenn eine Kennzahl kein Verhältnis angibt, sollten Sie sich genauer ansehen, wie die Risikovarianz gemessen wird.

Manchmal ist es auch gut, wenn eine Kennzahl ein erhöhtes Risiko anzeigt. Frühwarnsysteme sind ein Zeichen für ein gut funktionierendes Risikoteam, und Cyberrisiken sind dynamisch. Bestrafen Sie daher keine Metriken oder Teams, die ein erhöhtes Risiko anzeigen, da sie möglicherweise frühzeitig eine Botschaft für Sie darstellen.

Es gibt eine Reihe von Stichworten, die beschrieben, was gute Metriken ausmachen:

- Objektiv
- Unveränderlich
- Wiederholbar
- Kontinuierlich
- Relevant
- Wirksam
- Fundiert
- Vereinbart
- Umsetzbar

Ein Metrikmodell

Wir schlagen ein Metrikmodell mit den folgenden drei Schritten vor:

1. Sammeln Sie relevante Cyber-Hinweise
2. Transformieren Sie die Erkenntnisse in Geschäftsrisiken[18]
3. Informieren Sie den Vorstand, geben Sie angemessen Garantien und weisen Sie auf Lücken hin

In diesem Modell wird jeder Schritt in einzelne Bausteine zerlegt, die wir im Folgenden darstellen und kommentieren werden und für die in Anhang 2 Beispiele aus der Community aufgeführt sind. Ziel ist es, Anregungen und Einblicke für unternehmensspezifische Lösungen zu geben und nicht zu

[18] Das Geschäftsrisiko ist das Risiko, dem ein Unternehmen ausgesetzt ist und das seine finanziellen Ziele beeinträchtigt oder zu seinem Scheitern führen wird. Es gibt viele Arten von Geschäftsrisiken, z. B. strategische, operative, Reputations-, Compliance- oder finanzielle Risiken.

behaupten, wir würden eine perfekte Lösung für die Messung und Berichterstattung von Cyberrisiken vorschlagen.

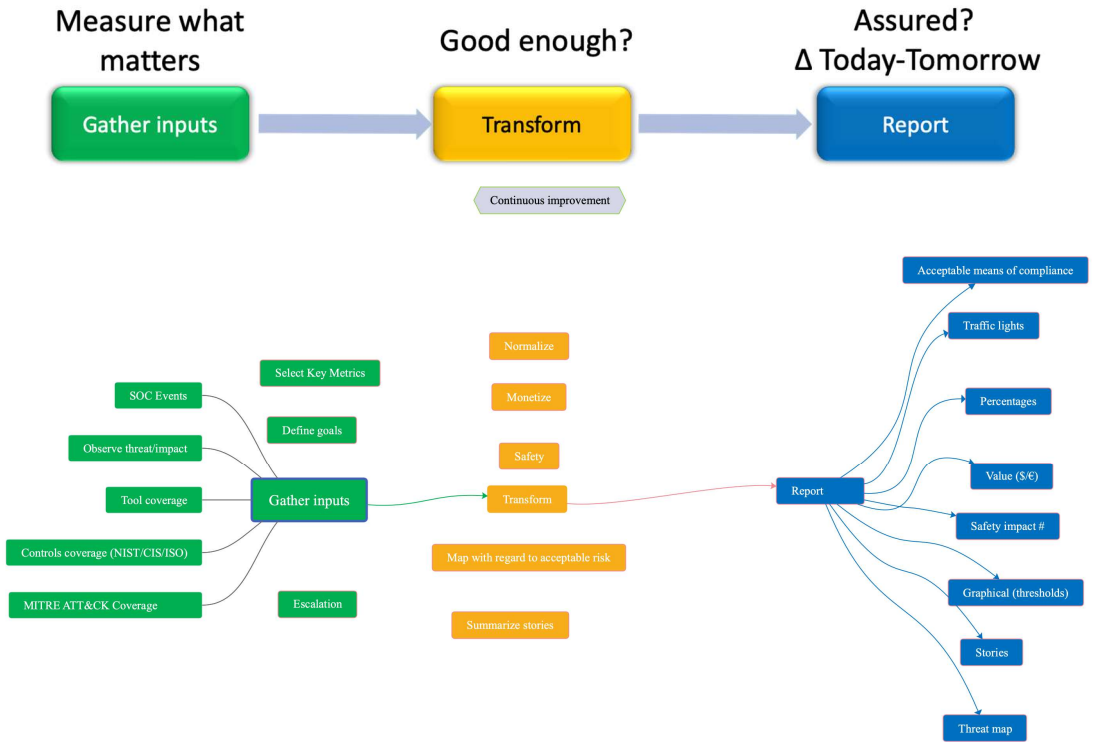


Abbildung 6 Metrikmodell

Verbesserungsschleifen (auf lokaler und übergreifender Ebene) sollten in das Metrikmodell und seine relevanten Prozesse integriert werden, um es an veränderte Erwartungen der Interessengruppen und an die Risikolage (Bedrohungslandschaft, Schwachstellen, Abhängigkeiten) anzupassen. Erkenntnisse und Methoden, die sich aus der Community ergeben, führen ebenfalls zu Verbesserungen.

Sammeln von Inputs – messen, was am wichtigsten ist

Auf der Eingabeseite des Metrikmodells finden wir technische Metriken, die (eine Teilmenge) derjenigen sein sollten, die vom Unternehmen / dem operativen Bereich zur Umsetzung und Überwachung der betrieblichen Cyber-Risikominderung verwendet werden. Unter Abbildung 7 finden wir diese technischen Metriken auf der unteren linken Seite des Diagramms.

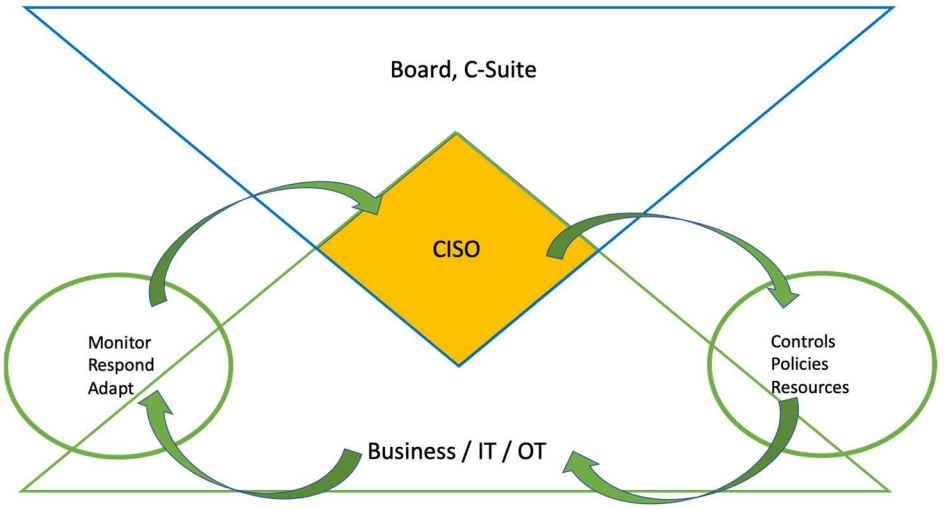


Abbildung 7 Technische Metriken - Eingaben

Abbildung 8 Sammeln von Inputs - Bausteine

Wir können verschiedene Familien operativer Kennzahlen unterscheiden, die wir nach ihrer Art gruppieren (**kontrollorientiert**, **gefahrenorientiert**, **toolorientiert** und **ereignisorientiert**).

Kontrollorientiert

In dieser Kategorie finden wir Metriken, die die Organisation ermittelt, um die Übereinstimmung mit einer Reihe von Schlüsselkontrollen zu messen. Diese beziehen sich auf einen Kontrollrahmen (NIST CSF, ISO, CIS, usw.).

Zu den kontrollorientierten Metriken könnten gehören:

- Abdeckung einer Kontrolle – für alle Vermögenswerte oder eine ausgewählte Gruppe der (wichtigsten) Vermögenswerte;
- Wirksamkeit einer Kontrolle;
- Datenquelle und Aktualisierungshäufigkeit;
- Schwellenwert.

Eine (detailliertere) Variante dieses kontrollorientierten Ansatzes teilt die Abdeckung einer Kontrolle in drei Komponenten auf: implementiert, funktionsfähig und wirksam. Es ist wichtig zu beachten, dass diese Messungen kontinuierlich erfolgen sollten, da sich die Bedrohungslandschaft und die Fähigkeit der Kontrolle, Risiken zu bewältigen, im Laufe der Zeit verändern. Diese drei Kontrollen werden wie folgt definiert:

- Bereitgestellt – ist die Kontrolle dort installiert, wo sie sein sollte;
- Funktionsfähig funktioniert die Kontrolle wie vorgesehen;
- Wirksam ist die Kontrolle wirksam, ein Maß („Beweis") dafür, ob eine bestimmte Kontrolle über einen bestimmten Zeitraum zur Risikominderung beiträgt.

Für jeden dieser drei Bereiche wird durch das Sammeln von Beweisen eine Punktzahl ermittelt. Eine kombinierte Bewertung der drei Bereiche ergibt einen „Abdeckungsgrad".

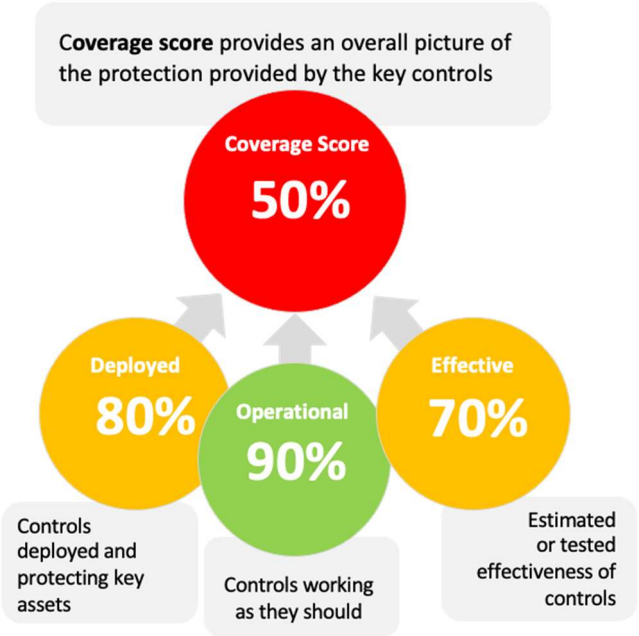


Abbildung 9 Beispiel für eine kontrollzentrierte Metrik bei einer Pandemie-Infektion

Ein praktisches Beispiel für dieses Konzept sind Pandemie-Infektionen, bei denen ein Impfstoff eine der möglichen Schlüsselkontrollen darstellt;

- Bereitstellung wäre der geimpfte Teil der Bevölkerung (in diesem Beispiel 80 %);

- Wenn der Impfstoff erst nach einer gewissen Zeit eine Immunreaktion hervorruft, führt dies zu einem Unterschied im Anteil der verabreichten Impfstoffe, die einsatzbereit sind (in diesem Fall 90 %);
- Ein Impfstoff ist nur bis zu einem bestimmten Grad wirksam (in diesem Fall 70 %);
- Daher beträgt in diesem Fall die Gesamtabdeckung 50 % (eine Kombination aus den drei Faktoren).

$$\eta = \frac{70}{100} \times \left(\frac{90}{100} \times 80\right)$$
$$\eta = 50.4$$

Die Wirksamkeit der Kontrollen könnte an einzelnen Kontrollen (Pentests) oder an allen eingesetzten Kontrollen (Red Teaming) getestet werden. Im letzteren Fall könnte das Ergebnis dazu verwendet werden, die Verringerung des Cyberrisikos insgesamt einzuschätzen.

Ein kontrollorientierter Ansatz ist in der Regel in stark regulierten Umgebungen zu finden. So wird beispielsweise von den Regierungsbehörden in den USA erwartet, dass sie NIST 800-53 umsetzen, das rund 1.000 Kontrollen und Kontrollverbesserungen umfasst.

Doch selbst in regulierten Umgebungen mit obligatorischen Kontrollen ist es sinnvoll, die Schlüsselkontrollen zu ermitteln, die für die Minderung des aktuellen Cyberrisikos am wichtigsten sind. Die Auswahl der Schlüsselkontrollen könnte durch das Verständnis der wichtigsten Bedrohungen (Motive und Techniken) und der wichtigsten Zielobjekte gefördert werden.

Einige Beispiele für kontrollorientierte Metriken

- K1: Prozentsatz der (wichtigsten) inventarisierten Vermögenswerte (Endpunkte, Netzwerk, Server);
- K1: Unverschlüsselte Datenbanken, die personenbezogene Daten speichern;
- K2: Prozentsatz der wichtigen Vermögenswerte, die mit der Sicherungsrichtlinie übereinstimmen;
- K4: Prozentsatz der Endpunkte ohne lokale Administratorrechte;
- K4: Prozentualer Anteil der Endpunkte mit implementiertem Anwendungs-Whitelisting;
- K4: Prozentsatz der privilegierten Konten, die von einer Zugangskontrolllösung verwaltet werden;
- K8: Prozentsatz der (wichtigen) Vermögenswerte, die mit dem Internet verbunden sind und wöchentlich auf Schwachstellen und Fehlkonfigurationen überprüft werden;
- K9: Prozentsatz der kritischen Anwendungen ohne Business-Impact-Analyse;
- K10: Prozentsatz der Mitarbeiter, die im vergangenen Jahr an einer Cybersicherheitsschulung teilgenommen haben (einschließlich der Vorstandsmitglieder);
- Wirksamkeit der Schlüsselkontrollen, die durch Red Team oder automatisierte Tests ermittelt werden.

Bedrohungsorientiert

In dieser Kategorie finden wir Metriken, mit denen die Organisation mithilfe des MITRE ATT&CK® Framework ihre wichtigsten Gegner identifiziert und die TTPs (Techniken, Taktiken, Prozeduren) verfolgt, die bekanntermaßen eingesetzt werden. Abhilfemaßnahmen werden ähnlich wie beim kontrollorientierten Ansatz auf diese Techniken abgestimmt. Dieses Wissen muss mit den neuesten Informationen über relevante Gegner und Vorfälle auf dem neuesten Stand gehalten werden.

In der nachstehenden Abbildung ist die Verwendung von Techniken durch verschiedene relevante Gegnergruppen farblich hervorgehoben, von gelb (weniger verbreitet) bis rot (von allen relevanten Gegnern verwendete Techniken).

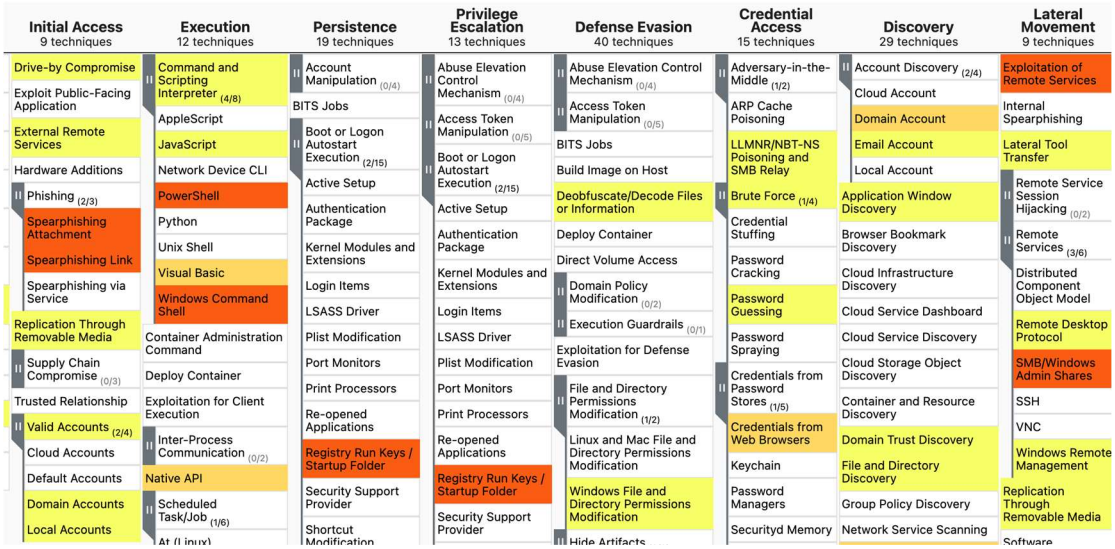


Abbildung 10 Beispiel für die Verwendung einer Heatmap zur Darstellung der Prävalenz von Techniken

Bedrohungsorientierte und kontrollorientierte Ansätze können kombiniert werden, indem Zuordnungen zwischen Kontroll- und Bedrohungsrahmen[19] verwendet werden, um ausgewählte relevante Bedrohungen und komplementäre Kontrollen zu identifizieren und in wichtige Kennzahlen umzuwandeln.

Einige Beispiele für bedrohungsorientierte Metriken:

- Prozentsatz der Abdeckung von Techniken, die bekanntermaßen von relevanten Angreifergruppen verwendet werden;
- Prozentsatz der Abdeckung der wichtigsten Abhilfemaßnahmen durch ein aktives Testprogramm (automatisiert oder Red Team);
- Prozentsatz der Abdeckung hinsichtlich relevanter Gegner und ihrer Techniken durch SOC-Playbooks und Hunting-Programme.

Werkzeugorientiert

In dieser Kategorie finden wir Metriken, bei denen sich die Organisation auf den Einsatz spezifischer Cybersicherheits-Tools (EDR, Perimeter-Verteidigung, MFA usw.) konzentriert, um eine Risikominderung zu erreichen. Die

[19] https://github.com/center-for-threat-informed-defense/attack-control-framework-mappings

Datenerfassung über den Einsatz von Tools ist unkompliziert und die Zuordnung der Wirksamkeit jedes Tools gegenüber bekannten Bedrohungen ist ebenfalls gut dokumentiert.

Es könnten ähnliche Grundsätze wie beim kontrollorientierten Ansatz angewandt werden, z. B. Abdeckung/Wirksamkeit oder implementiert/funktionsfähig/ausführbar. Ein werkzeugorientierter Ansatz könnte ein Sprungbrett für einen kohärenteren und umfassenderen Ansatz auf der Grundlage eines Rahmenwerks (kontroll- oder bedrohungsorientiert) sein.

Einige Beispiele für werkzeugorientierte Metriken sind:

- K3: Prozentsatz der Umsetzung der Multi-Faktor-Authentifizierung (MFA);
- K6: Prozentsatz der Systeme mit vollständiger Suite von Sicherheitswerkzeugen und -richtlinien (EDR, Protokollierung, Goldstandard-Software und -Konfiguration, Richtlinien usw.);
- K6: Prozentsatz der (wichtigen) Vermögenswerte mit transparenter Protokollierung;
- K8: Prozentsatz der Vermögenswerte, die über einen Proxy auf das Internet zuzugreifen müssen;
- Prozentsatz der Vermögenswerte, die durch automatische Kontrollen und Abhilfemaßnahmen geschützt sind.

Ereignisorientiert

Viele Unternehmen sammeln Daten über Cybersecurity-Ereignisse (#Alarme, #Vorfälle, #falsch positive Meldungen, #Schwachstellen usw.). Solche Statistiken können einen wertvollen Beitrag zum Management von Cybersicherheitsrisiken leisten, aber sie müssen interpretiert werden. Ist es gut oder schlecht, wenn mehr Schwachstellen gefunden werden oder sich mehr Vorfälle ereignen? Haben sich die Erkennungsmethoden verbessert oder haben sich die Systeme verschlechtert?

Einige Beispiele für ereignisorientierte Metriken sind:

- K1: Anzahl der implementierten Sicherheitssysteme im Verhältnis zur Abdeckung der Vermögenswerte;
- K4: Anzahl der Probleme, die bei der Überwachung/Überprüfung privilegierter Vermögenswerte festgestellt wurden;
- K5: Prozentsatz der innerhalb von SLAs gepatchten Systeme;
- K6: Anzahl der Fehlalarme im Security Operation Center;
- K8: Anzahl der gefundenen (nach außen gerichteten) verwaisten Vermögenswerten;
- K9: Anzahl der kritischen Zwischenfälle/durchschnittliche Zeit bis zur Entdeckung/Eindämmung;
- K9: Prozentsatz der kritischen und Hochsicherheitswarnungen, die innerhalb der SLAs überprüft werden;
- K10: Anzahl der Unternehmensanmeldedaten „In the Wild" (Kontoübernahme);
- Jährliche Kosten von Cyber-Vorfällen;

- Anzahl der offenen Sicherheits- und Datenschutzprobleme mit hohem Risiko, die außerhalb der SLAs liegen und für die kein Abhilfeplan vorliegt.

Zeitliche Daten über Vorfälle und Schwachstellen können nützliche Informationen über die Leistung der Cybersicherheitsorganisation und ihrer Systeme liefern. In der First Metrics SIG[20] wurden gute Fortschritte zu diesem Thema erzielt.

Risiko in der Lieferkette

Immer mehr Unternehmen bekommen die Auswirkungen von Cybervorfällen zu spüren, die ihre Zulieferer betreffen, entweder direkt durch Netzwerkverbindungen oder Produkte oder indirekt durch Unterbrechungen der Lieferkette, die die Geschäftskontinuität beeinträchtigen. Die Erfassung der Abhängigkeiten von Zulieferern, die Gewinnung von Erkenntnissen über deren Cybersicherheitslage und die Implementierung geeigneter Kontrollen werden zu einem integralen Bestandteil des Cyber-Risikomanagements und sollten daher auch in die Messgrößen einbezogen werden.

Die Überwachung des Cyberrisikos von Zulieferern kann von spezialisierten Unternehmen übernommen werden. Abhilfemaßnahmen können bis zu einem gewissen Grad in Form von Vertragsbedingungen und über eine Versicherungsschutz getroffen werden. Es sollte jedoch ein klares Bild der Abhängigkeiten und Szenarien für die Erkennung und Reaktion erstellt werden. Weitere Hinweise finden sich in der NIST-Publikation „Key Practices in Cyber Supply Chain Risk Management"[21] .

Einige Beispiele für Metriken der Lieferkette sind:

- Prozentsatz der kritischen Anbieter/Lieferanten, für die eine Bestandsaufnahme der Vermögenswerte, der Abhängigkeiten, der Risikobewertung und -minderung durchgeführt wurde;
- Prozentsatz der kritischen Anbieter/Lieferanten mit Sicherheitsanhängen;
- Prozentsatz der kritischen Lieferanten, die geprüft wurden;
- Anzahl der kritischen Anbieter/Lieferanten mit offenen, hohen Sicherheits- und Datenschutzrisiken ohne dokumentierten Risikomanagementplan, die im Rahmen von Prüfungen festegestellt wurden.

Auswirkungen beobachten – Erzählungen

Viele Organisationen dokumentieren relevante Vorfälle (intern, mit Auswirkungen auf Peers, den Sektor oder die Region) anhand von Narrativen in „Erzählungen". Diese Art von anekdotischer Evidenz spricht Mitglieder der Unternehmensführung und des Vorstands ohne technischen Hintergrund an, da sie beispielhaft veranschaulichen, was der Organisation passieren kann (oder passiert ist). Sie ermöglichen es dem CISO auch, die Aufmerksamkeit auf Trends in Bezug auf Häufigkeit, Auswirkungen und Methoden in der

[20] https://www.first.org/global/sigs/metrics/events
[21] https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

Bedrohungslandschaft zu lenken, und unterstützen die Priorisierung von Maßnahmen in Bezug auf Kontrollen und Ressourcenzuweisung.

Sorgfältige Auswahl wichtiger Kennzahlen und Ziele

Schlüsselkennzahlen müssen sorgfältig ausgewählt werden, denn die Auswahl und die Berichterstattung über die Kennzahlen sind für eine Organisation entscheidend. Aus der Auswahl der Kennzahlen lässt sich ableiten, was für die Unternehmensführung am wichtigsten ist und woran Mitarbeiter sich orientieren werden. Werden die falschen Dinge gemessen, werden die angestrebten Cybersicherheitsziele verfehlt und es kommt zu falschen Annahmen über die Risikolage. Darüber hinaus möchte der Vorstand möglicherweise seine Aufmerksamkeit auf die Verbesserung der Indikatoren und nicht auf die zugrundeliegende Cyber-Risikolage richten.

Schlüsselkennzahlen sollten sich im Laufe der Zeit mit der zunehmenden Reife der Organisation, den Änderungen der gesetzlichen Anforderungen, den Geschäftszielen und den Veränderungen in der Cyber-Bedrohungslandschaft weiterentwickeln. Für die ausgewählten Metriken müssen Ziele festgelegt und innerhalb der Organisation vereinbart werden. Diese müssen im Hinblick auf die Risikominderung und die Risikobereitschaft sinnvoll sein. Sie könnten eine zeitliche Komponente enthalten, falls die Organisation eine Entwicklung des Reifegrads im Laufe der Zeit berücksichtigen möchte.

Eskalationsprozess

Es wird empfohlen, einen Prozess/Schwellenwert zu definieren, der eine Notfallmeldung über Abweichungen/Entwicklungen an die Führungsebene zwischen den Berichtszeiträumen auslöst. Dabei können nicht nur kritische Vorfälle/Verletzungen Auslöser sein, sondern auch bedeutende Schwachstellen oder Entwicklungen in der Bedrohungslandschaft, die sofortige Aufmerksamkeit der Führungsebene erfordern. Ein aktuelles Beispiel für einen solchen Fall war die Log4j-Schwachstelle und die Abhängigkeit vieler Unternehmen von Produkten, die diese Softwarekomponente verwenden.

Ein Eskalationsprozess könnte auch für Kennzahlen entwickelt werden, die nur dann an den Vorstand gemeldet werden, wenn ein vordefinierter Schwellenwert überschritten wird. Dies könnte die Überlastung des Vorstands mit irrelevanten Informationen verringern.

Datenquellen – eine unwiderlegbare Wahrheit

Intern gesammelte Daten

Technische Metriken sollten aus Daten bestehen, die automatisch und mit minimaler menschlicher Beteiligung von der Quellinfrastruktur erfasst werden. Dazu gehören:

- Asset-Management- und Discovery-Systeme (Vollständigkeit, Kritikalität);
- Systeme zum Toolmanagement und Konsolen (Bereitstellung);
- Logs und SIEMs (Bereitstellung und Betrieb);
- Scannen von Software (Versionen, Schwachstellen, Konfigurationen, Richtlinien);

- Identitäts-, Berechtigungs- und Zugriffsmanagement (Kontrollen und Richtlinien);
- Netzwerkspuren (Vollständigkeit, Kontrollen).

Die meisten dieser Daten beziehen sich auf den Einsatz von Kontrollen, Instrumenten und Strategien. Die Wirksamkeit der Risikominderung lässt sich theoretisch auf der Grundlage der erwarteten Minderung durch eine bestimmte Kontrolle ableiten.

Aus Tests gewonnene Daten

Zusätzliche Erkenntnisse über die Implementierung (Bereitstellung und Betrieb), insbesondere über die Wirksamkeit, können durch Tests der Kontrollen gewonnen werden. Typischerweise können solche Tests von Kontrollen durch Pentests/Red Teaming oder automatisierte Tests mit speziellen Tools oder Bug Bounty-Programmen durchgeführt werden. Diese Kategorie von Metriken ist vor allem in Unternehmen sinnvoll, die bereits über ein ausgereiftes Informationssicherheitsmanagementsystem[22] verfügen.

Außerhalb der Infrastruktur erhobene Daten

Einige Daten über bestätigte Infektionen und Schwachstellen können von außerhalb der Infrastruktur eines Unternehmens gesammelt werden, indem Netzwerkspuren gescannt oder beobachtet werden, die auf bekannte bösartige Infrastrukturen verweisen.

Transformation – Sind unsere Kontrollen ausreichend?

Während wichtige operative Kennzahlen für den CISO wichtig sind, um die Umsetzung der Cybersicherheitsstrategie zu steuern und die Kontrollen detailliert zu überwachen, eignen sie sich nicht für die Berichterstattung an die Geschäftsleitung, den Vorstand und andere strategische Interessengruppen. Sie würden als überwältigend, kryptisch und losgelöst vom Geschäftsrisiko wahrgenommen werden.

Damit die Metriken für Cyberrisiken auf Vorstandsebene Gehör finden, müssen sie in aussagekräftige Geschäftsberichte (Geld, Sicherheit, Markenwert usw.) umgewandelt und mit der Risikobereitschaft verglichen werden. Ist unsere Risikominderung ausreichend? Können wir eine angemessene Sicherheit bieten? Kann der Vorstand unsere Annahmen und Orientierungen bestätigen? Die folgende Abbildung zeigt den Informationsfluss von den technischen/operativen Kennzahlen zu den Vorstandskennzahlen.

[22] https://www.iso.org/isoiec-27001-information-security.html

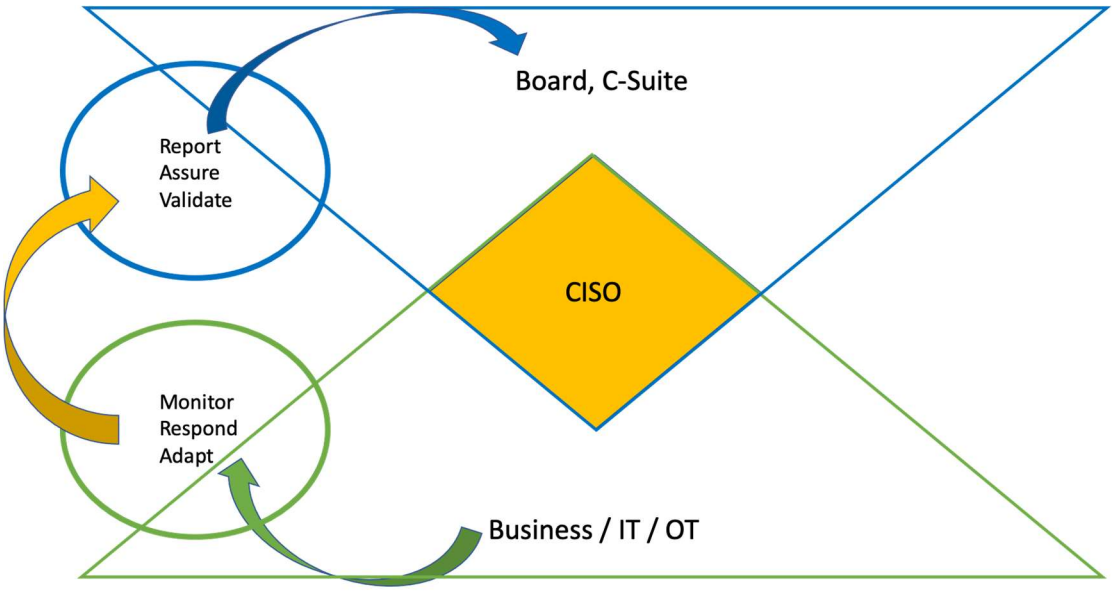


Abbildung 11 Umwandlung technischer Metriken in strategische Metriken

Auch hier unterscheiden wir eine Reihe von Bausteinen in der Transformationsphase. Diese wandeln operative Schlüsselkennzahlen in Werte um, die mit dem tolerierbaren Risiko verglichen, in das Geschäftsrisiko integriert und dem Vorstand gemeldet werden können.

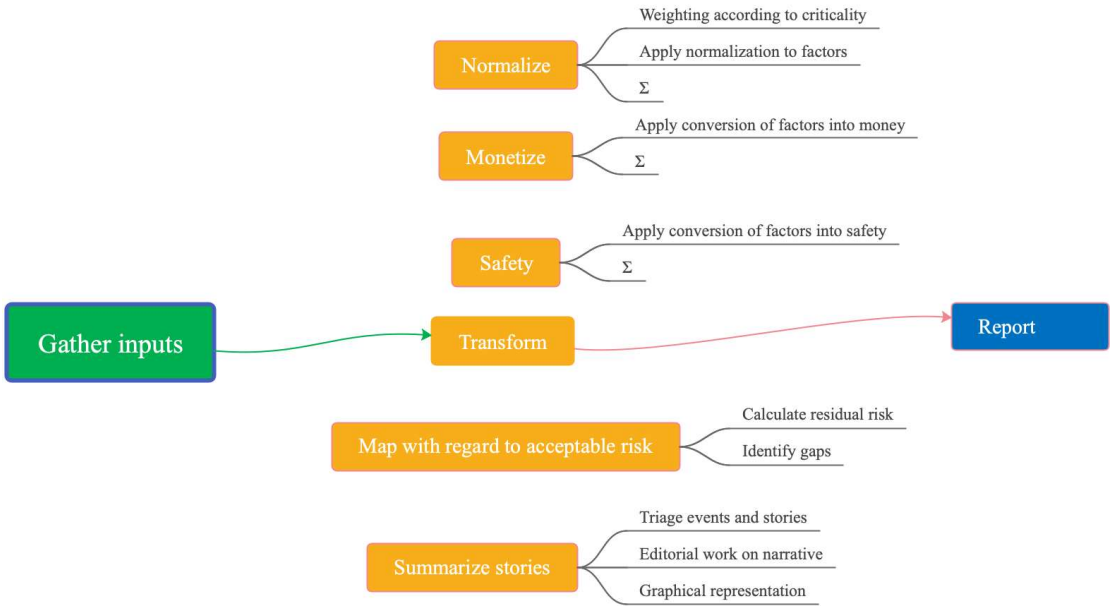


Abbildung 12 Transformieren - Bausteine

Normieren

In jeder Organisation kann es eine große Anzahl von Kennzahlen geben, die den Zustand der Kontrollen und die Leistung der Organisation beschreiben. Dies kann den negativen Effekt haben, dass die Beteiligten von den Details überwältigt werden. Ein weiteres Problem besteht darin, dass der Wert einer einzelnen Messung für sich genommen bedeutungslos sein kann, wenn er unabhängig betrachtet wird, aber kritisch wird, wenn er über eine Reihe von Metriken betrachtet wird.

Wenn Sie zum Beispiel den Schutz Ihrer Endgeräte vor Malware verstehen wollen, reicht es nicht aus, nur den Einsatz von Antivirensoftware auf einem bestimmten Betriebssystem zu betrachten. Sie müssen die verschiedenen Messungen für die verschiedenen Betriebssysteme betrachten. Darüber hinaus liefert Antiviren-Software allein keine Antwort. Sie müssen auch die Messungen anderer Tools wie Event Detection Response (EDR) betrachten.

Um diese Herausforderung zu bewältigen, können verschiedene Metriken, auch wenn sie unterschiedlicher Natur sind, normiert oder harmonisiert werden, um einen ganzheitlicheren Überblick zu erhalten. Eine solche Normierung sollte eine vereinfachte Sicht auf eine große Anzahl unterschiedlicher Kontrollbereiche ermöglichen und gleichzeitig Einblicke in wichtige Lücken geben, die durch eine Konsolidierung verschleiert werden könnten.

Die Normierung könnte auch eine Gewichtungskomponente enthalten, um den unterschiedlichen Kritikalitätsgraden der Vermögenswerte Rechnung zu tragen. So könnte beispielsweise die Abdeckung der Kontrollen von äußerst kritischen Vermögenswerten als wichtiger bewertet werden als in anderen. In einer konsolidierten Kennzahl könnte dies durch Gewichtung berücksichtigt werden.

Mit Hilfe einer dreistufigen (rot/gelb/grün) Min-/Max-Skalierungsnormierung ist es möglich, die Metrik einer neuen Skala zuzuordnen, wobei das genaue Verhältnis innerhalb jeder Stufe beibehalten wird (d. h. eine Eingabemetrik, die am oberen Ende von Rot liegt, bleibt am oberen Ende von Rot, auch wenn sich ihr numerischer Wert ändern kann).

In dieser Grafik werden mehrere Metriken auf niedriger Ebene auf eine gemeinsame Skala normiert. Sobald sie auf eine gemeinsame Skala normiert sind, können diese Metriken sinnvoll aggregiert oder kombiniert werden, und diese Aggregationen können kaskadiert werden, um nur einige wenige zusammengefasste Metriken auf oberster Ebene zu erhalten.

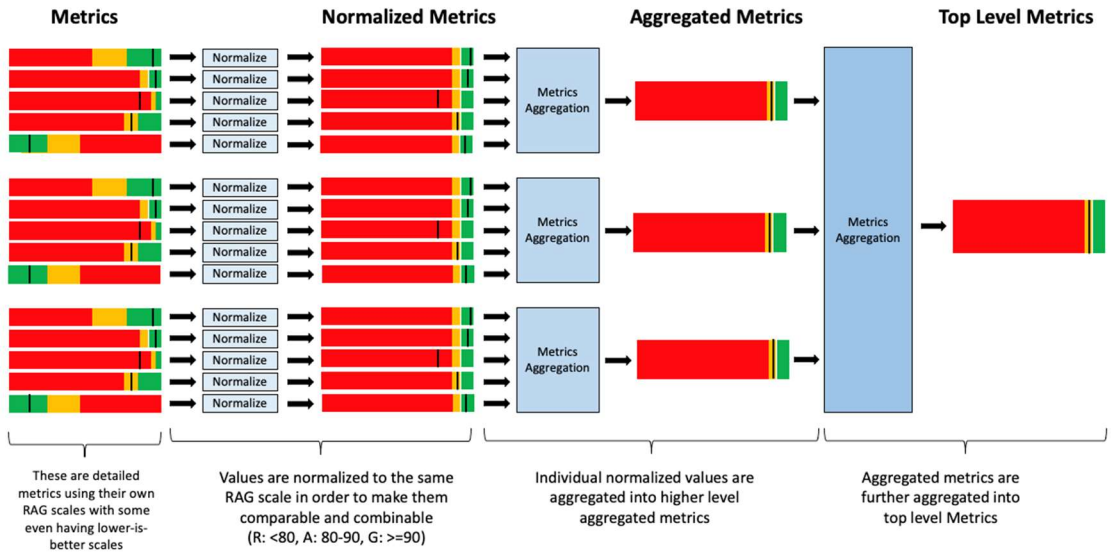


Abbildung 13 Dreistufige (rot/gelb/grün) Min-/Max-Skalierungsnormierung

Monetarisieren (Value at Risk)

In Unternehmen wird die Risikobereitschaft in monetären Größen ausgedrückt. Daher muss versucht werden, die Metriken so umzuwandeln, dass sie von den wichtigsten Interessengruppen verstanden werden können, um eine praktikable Anwendung innerhalb der normalen Geschäftsprozesse zu ermöglichen. Dies ist besonders wichtig, wenn es um die Beantragung von Finanzmitteln geht. Wenn die Cybersicherheitsabteilung beispielsweise 10 Mio. USD für die Einführung eines neuen EDR-Systems benötigt, ist die Feststellung, dass dadurch das aktuelle Risiko für das Unternehmen um 12 Mio. USD verringert wird und das Unternehmen wieder innerhalb der Risikobereitschaft liegt, eine starke Rechtfertigung.

In diesem Schritt werden einzelne oder aggregierte betriebliche Kennzahlen in den Wert des verwalteten Risikos umgerechnet. Im Hinblick auf den Wert müssen wir die direkten Auswirkungen eines Vorfalls auf das Unternehmen (Kontinuität des Betriebs, Rechtsstreitigkeiten mit Kunden, Strafen bei Verstößen gegen Vorschriften, Kosten für die Reaktion auf den Vorfall, Ransomware-Zahlungen) sowie die indirekten Auswirkungen (Schaden für das Markenimage, Aktienkurs) berücksichtigen.

Eine der Methoden zur Monetarisierung ist die Factor Analysis of Information Risk (FAIR™) [23] , ein Modell zum Verständnis, zur Analyse und zur Quantifizierung von Cyberrisiken und operationellen Risiken in finanzieller Hinsicht. Diese Methode ist gut etabliert und wurde ausführlich veröffentlicht. Für kleinere oder weniger ausgereifte Organisationen kann sie jedoch zu aufwändig und schwer zu pflegen sein.

Der PHOSI-Rechner (Potential Harm of Security Incident) des niederländischen Telekommunikationsanbieters KPN ist eine kostengünstige Alternative, die als App auf Smartphones verfügbar ist[24][25]. Er erleichtert die Berechnung des Werts im Risiko anhand einer kleinen Anzahl von Fragen. Diese PHOSI-Schätzungen können mit einzelnen Bedrohungen/Kontrollen oder auch mit Ergebnissen aus dem Red Teaming (welcher potenzielle Schaden wurde durch rechtzeitiges Patchen einer kritischen Schwachstelle oder durch eine Red Team-Übung vermieden?) oder der Exposition gegenüber wichtigen Schwachstellen kombiniert werden.

Eine umfassendere und einfachere Möglichkeit zur Monetarisierung wichtiger operativer Kennzahlen besteht darin, das Ergebnis der Normierung/Konsolidierung als Minderungsfaktor zu verwenden, der mit der durchschnittlichen Häufigkeit und den Auswirkungen eines in der Community beobachteten Cybervorfalls multipliziert wird. Forschungsarbeiten zur Häufigkeit und zu den Auswirkung von Ransomware-Vorfällen haben interessante Beispiele für solche Näherungswerte ergeben [26] . Neuere

[23] https://www.fairinstitute.org/what-is-fair
[24] https://apps.apple.com/us/app/kpn-ciso/id1122223795
[25] https://play.google.com/store/apps/details?id=com.kpn.ksp&hl=en&gl=US
[26] https://www.youtube.com/watch?v=kSi-oXq4xV0

wissenschaftliche Arbeiten in diesem Bereich finden sich auch in „A System to Calculate Cyber-Value-at-Risk“[27].

Es ist wichtig, darauf hinzuweisen, dass dies ein aktiver Forschungsbereich ist und die Methoden zur Quantifizierung des Risikos nicht perfekt sind. Auch wenn dies ein anzustrebendes Ziel ist und für die Kommunikation mit den wichtigsten Interessengruppen wichtig ist, sollten die Ergebnisse mit Vorsicht behandelt werden.

Auswirkungen auf die Sicherheit (Life at Risk)

Einige Organisationen sind aufgrund ihrer Tätigkeit nicht nur mit den finanziellen Auswirkungen, sondern auch mit den Auswirkungen auf die Sicherheit befasst. Dies ist der Fall bei Fluggesellschaften/im Flugverkehrsmanagement, Automobilherstellern, Krankenhäusern, Kernenergieversorgern usw.

Cyberrisiken, die zum Verlust von Menschenleben führen könnten, sollten abgeschätzt und die Wirksamkeit von Kontrollen und der Risikominderung gemessen und kontrolliert werden. In diesem Bereich wurden weitaus weniger Arbeiten veröffentlicht, aber das zugrundeliegende Prinzip wäre ähnlich wie die Berechnung des Werts im Risiko.

Dies ist sicherlich ein Bereich, in dem sich Organisationen weniger wohl dabei fühlen würden, Einschätzungen zu teilen oder Kompromisse und kalkulierte Risiken offenzulegen. Wird von außen wahrgenommen, dass eine Organisation Risiken für den Verlust von Menschenleben in Kauf nimmt, könnte dies sehr schnell zu einer Schädigung des Markenimages führen.

Da die Monetarisierung des Verlustes von Menschenleben nicht akzeptabel ist (zumindest in einigen Regionen der Welt), wird das akzeptable Risiko des Verlustes von Menschenleben mit einer Mischung aus quantitativen und qualitativen Mitteln zur Risikoberechnung bewertet, mit dem Ziel, so weit wie vernünftigerweise praktikabel und von den Vorschriften toleriert, kein Menschenleben zu verlieren.

Zuordnung zur Risikobereitschaft

Die Ergebnisse der Value/Life at Risk-Bewertungen müssen mit der Risikobereitschaft der Organisation verglichen werden. In vielen Organisationen ist diese Risikobereitschaft bereits im Rahmen der Geschäftsrisikoprozesse festgelegt worden. Sollte dies nicht der Fall sein, sollte der CISO das Unternehmen bzw. den Vorstand auffordern, die Risikobereitschaft zu bestimmen:

- Wie viel sind wir bereit zu verlieren, wenn Risiko eintritt?
- In welchem Umfang soll das Risiko gemindert werden?
- Wie viele Ressourcen sind wir bereit, für die Schadensbegrenzung zur Verfügung zu stellen?
- Versichern wir einen Teil des Risikos?

Einige werden wahrscheinlich argumentieren, dass es nicht möglich ist, die Wahrscheinlichkeit eines Verstoßes zu bewerten. Wir müssen jedoch bedenken,

[27] https://www.sciencedirect.com/science/article/pii/S0167404821003692

dass niemand versuchen wird, die Wahrscheinlichkeit zu quantifizieren, wenn es keinen Richtwert für die Risikobereitschaft gibt. Wir plädieren dafür, eine Diskussion über die Risikotoleranz anzustoßen, wie z. B. „weniger als 5 % Chance pro Jahr, dass der Schaden durch eine Cyberverletzung 1 Million Dollar übersteigt". Wir verstehen, dass ein derartiger quantitativer Ansatz für Cyberrisiken schwer umsetzbar und eher die Ausnahme als die Norm ist. Es handelt sich jedoch um ein ehrgeiziges Ziel, eine Risikoquantifizierung zu erreichen und angemessene Budgets zu ermöglichen.

Stellen Sie zunächst falsche Berechnungen an und lassen Sie die Führungskräfte daran arbeiten, die Frage mit einer wiederholbaren Methode zu beantworten. Wenn Sie keine Ahnung haben, welche Zahlen Sie verwenden sollen, prüfen Sie andere Risiken in Ihrem Unternehmen, z. B. die Risikotoleranzen für Feuer, Überschwemmung oder Arbeitsunfälle. Es kann sich dabei um sehr unterschiedliche Risiken handeln, aber sie können Ihnen einen Anhaltspunkt dafür geben, wie Sie die von Ihnen angestrebte Risikotoleranz ausdrücken können. Vielleicht stellen Sie am Ende fest, dass das Risiko für Ihr Unternehmen tatsächlich eher bei 10 % liegt, aber dann wird die Diskussion darüber, wie viel es kostet, es zu verringern, nachvollziehbar und rational.

Die Zuordnung von Value/Life at Risk zur Risikobereitschaft ist notwendigerweise eine mehrdimensionale Analyse, bei der die erwartete Häufigkeit und die möglichen Auswirkungen kombiniert werden und bei der die aktuelle Situation in einer Reihe von Datenpunkten auf der Grundlage von Hypothesen über die Wirksamkeit der Kontrollen ausgedrückt werden könnte.

Die Zuordnung kann auch dazu verwendet werden, Verbesserungsmöglichkeiten im Zusammenhang mit vorgeschlagenen Kontrollen/Investitionen aufzuzeigen. Nichts davon wird jedoch wahrscheinlich geschehen, wenn der Vorstand nicht von vornherein eine Risikotoleranz festlegt. Erst dann können Diskussionen über die Realitätsnähe der Zahlen und die Erwartungen an die Widerstandsfähigkeit gegenüber Cyberrisiken geführt werden.

Geschichten zusammenfassen

Die Auswahl relevanter Informationen (Vorfälle innerhalb und außerhalb des Unternehmens, Informationen über Cyber-Bedrohungen, Entwicklungen im Bereich der Rechtsvorschriften) und die Herausarbeitung des Kerns (warum ist dies relevant?) ist eine wesentliche Ergänzung zu den quantitativen Kennzahlen.

Die Eingrenzung der Erzählung und die Darstellung einer überzeugenden Geschichte erfordern besondere Fähigkeiten des CISO und seines Teams. Ausgewählte Geschichten müssen einen zusätzlichen Kontext zur Risikolage des Unternehmens liefern und einem bestimmten Zweck dienen. Andernfalls besteht die Gefahr, dass sie die Aufmerksamkeit ablenken und Energie und Ressourcen binden, die an anderer Stelle besser eingesetzt werden könnten.

Berichterstattung über Cyberrisiken – hinreichende Sicherheit bieten

Die Cyber-Berichterstattung an den Vorstand sollte dazu dienen, dem Vorstand (erneut) zu versichern, dass das Cyberrisiko heute und in Zukunft im Rahmen der Risikobereitschaft liegt:

- Sind wir gut genug?
- Sind die für den Cyberbereich bereitgestellten Ressourcen angemessen und wirksam?
- Wie schneiden wir im Vergleich zu unseren Mitbewerbern und unserem Sektor ab?

Da der Vorstand und seine Ausschüsse nicht auf Cyberfragen spezialisiert sind, wäre es ratsam, den Vorstand dabei zu unterstützen, die richtigen Fragen zu stellen und ihn nicht mit Informationen zu überhäufen. Um die Situation mit Bildern zu vergleichen, zeigt das nächste Bild ein „CISO"-Cockpit mit operativen Instrumenten und Konsolen, die es den Piloten ermöglichen, das Flugzeug zu steuern, um die Passagiere sicher und pünktlich an ihr Ziel zu bringen.

Abbildung 14 Quelle: Aeropers / Piloten von Swiss

Das folgende Bild zeigt ein „Vorstands"-Cockpit mit verschiedenen Instrumenten und ohne Steuerungsmöglichkeit, das vollständig von der Bodenkontrolle abhängig ist.

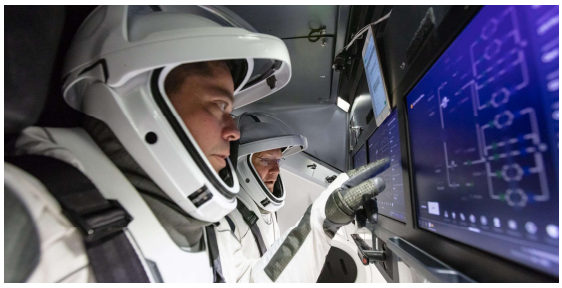


Abbildung 15 Quelle: NASA/SpaceX

Der Vorstand erwartet, dass der CISO alle Entwicklungen anzeigt, die die Situation wesentlich zum Besseren oder Schlechteren verändern würden, und entsprechende Maßnahmen und Ressourcen vorschlägt.

Die Festlegung eines Pakets von Cyber-Metriken und die konsistente Berichterstattung an den Vorstand, die einzelnen Mitglieder und die

zuständigen Ausschüsse (Audit, Compliance) kann eine wirksame und zuverlässige Methode sein, um Sicherheit im Bereich Cyber zu schaffen.

Sie kann mit der Berichterstattung über andere Arten von Geschäftsrisiken und mit der Berichterstattung über die Strategie der digitalen Transformation kombiniert/abgestimmt werden.

Metriken und Erzählungen

Das alte Sprichwort „ein Bild sagt mehr als tausend Worte" gilt auch im Zusammenhang mit der Einbindung Ihres Vorstands in die Cyberarbeit. In der Community wird eine große Vielfalt an grafischen Darstellungen von Cyber-Metriken verwendet, und die Betrachtung solcher Beispiele und der Austausch mit Branchenkollegen kann bei der Gestaltung des Berichtspakets einer Organisation sehr inspirierend sein. Unter Abbildung 16 haben wir einige Bausteine aufgenommen, die auf Beispielen aus der Community basieren und in den Anhängen enthalten sind.

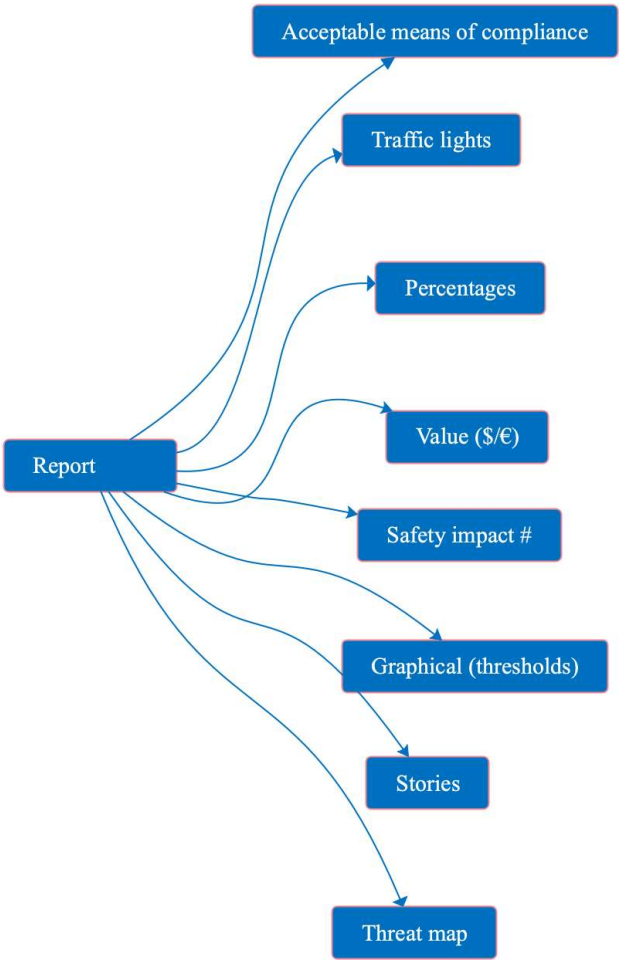


Abbildung 16 Berichterstattung - Bausteine

Kommunikationskanäle

Idealerweise würde eine Organisation einen kohärenten und integrierten Kommunikationskanal einrichten, um Ideen zu sammeln, umzuwandeln und dann dem Vorstand Bericht zu erstatten. Die Kommunikationsflüsse in Abbildung 17 würde wie beabsichtigt umgesetzt werden. Dies setzt voraus,

dass verschiedene Funktionen zusammenarbeiten und sich auf den Rahmen, die Prozesse zur Erfassung der Kennzahlen und die Rollen und Verantwortlichkeiten bei der Berichterstattung abstimmen.

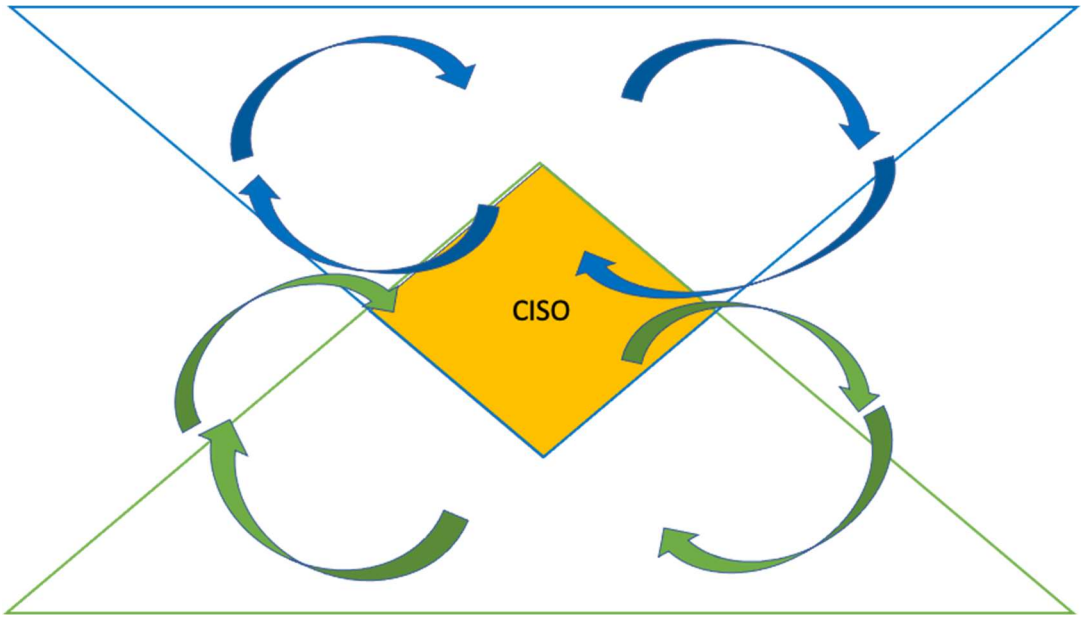


Abbildung 17 Optimaler Kommunikationsfluss

Unabhängig davon, wer dem Vorstand tatsächlich Bericht erstattet, muss der CISO eine Schlüsselrolle in diesem Prozess spielen und eine professionelle und unabhängige Sicht auf das Cyberrisiko gewährleisten. Im Optimalfall ist es der CISO, der dem Vorstand persönlich Bericht erstattet, was eine bessere Zusammenarbeit ermöglicht und die Zusicherung personifiziert.

Alternative Situationen, wie sie in Abbildung 18 dargestellt sind, in denen im ersten Diagramm keine Informationen an den Verwaltungsrat übermittelt werden, im mittleren Diagramm die dem Verwaltungsrat übermittelten Informationen nicht auf der Realität beruhen oder im dritten Diagramm dem Verwaltungsrat über verschiedene Kanäle widersprüchliche Informationen übermittelt werden, sind zu vermeiden oder einzustellen.

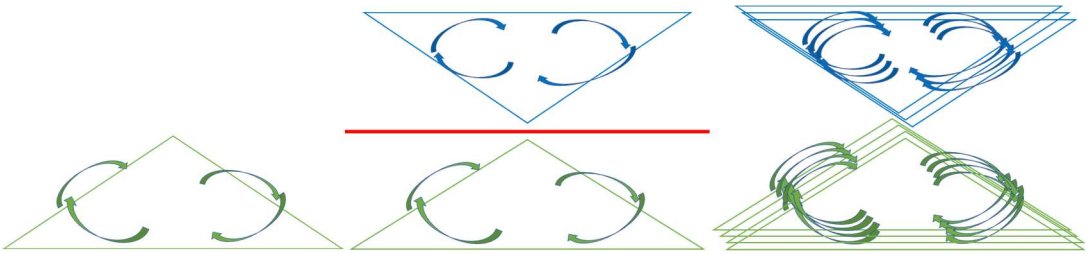


Abbildung 18 Inexistente, unverbundene, parallele Kommunikationsflüsse

Überwindung von Widerständen

Die im vorliegenden Dokument beschriebenen Konzepte werden zwar in gewissem Umfang bereits von Cybersicherheitsabteilungen verwendet, sie bilden aber auch eine Grundlage für die Integration von Cybersicherheitsrisiken als Teil der Risikomanagementprozesse des Unternehmens. Allerdings sind

diese Wechselwirkungen in vielen Organisationen immer noch eine Herausforderung:

- Cybersicherheit und Risiko werden von verschiedenen Abteilungen/Silos verwaltet;
- Cybersicherheit wird von den Geschäftsabteilungen als eine Disziplin für Insider, eine „schwarze Kunst", betrachtet;
- Risikomanagementmodelle werden von Cybersicherheitsabteilungen als komplex und abstrakt angesehen;
- Cyber-Vokabular und Metriken werden nicht in Geschäftsbegriffe übersetzt.

Um das Thema Cybersicherheit auf die Tagesordnung des Vorstands zu setzen, bedarf es einiger Anstrengungen und Überzeugungsarbeit, die jedoch durch eine Reihe von vorausschauenden Initiativen erleichtert werden kann:

- Verständnis für die Erwartungen des Vorstands und seiner einzelnen Mitglieder und Anpassung an sich ändernde Erwartungen;
- Sitzungen zur Sensibilisierung mit dem Vorstand, in denen Bedrohungen und Risiken auf verständliche Weise erläutert werden;
- Übungen zur Reaktion auf Zwischenfälle, an denen das Gremium beteiligt ist;
- Monatliche Übermittlung von Cyber-Briefs mit relevanten Informationen und Zusammenhängen an den Vorstand;
- Bilaterale Briefings mit einzelnen Vorstandsmitgliedern, die daran interessiert sind;
- Schrittweise Einführung und Verbesserung des Systems im Laufe der Zeit (z. B. Beginn mit der Umsetzung eines auf einem Reifegradmodell basierenden Ansatzes vor der Implementierung eines umfassenden quantitativen Modells);
- Transparente und positive Zusammenarbeit mit dem Prüfungsausschuss.

Zuweisung von Ressourcen für Metriken und die Berichterstattung

Es besteht kein Zweifel daran, dass die Einführung und Pflege eines Mess- und Berichterstattungssystems, wie es in diesem Dokument beschrieben wird, spezielle Ressourcen erfordert. Es spart jedoch auch Ressourcen durch interne Anpassungen/Optimierungen, durch die Vermeidung unnötiger reaktiver Medienreaktionen und letztlich durch die Konzentration der Ressourcen auf das, was wirklich wichtig ist, um das Cyberrisiko auf ein akzeptables Niveau zu reduzieren, wodurch Reaktionen auf Vorfälle und negative Auswirkungen vermieden werden.

Anhang 1: Erste Schritte

Fragen, die der Vorstand stellen sollte

- Verfügen wir über ein Inventar der wichtigsten Vermögenswerte?
- Wer hat es auf uns abgesehen (Hauptgegner) und warum?
- Welche sind unsere wichtigsten Kontrollen und welchen Status haben sie?
- Wo sind Lücken und wie wollen wir sie schließen?
- Verfügen wir über einen Plan für die Reaktion auf Zwischenfälle / Geschäftskontinuität / Widerstandsfähigkeit?
- Wie viel ist gefährdet?
- Wie schneiden wir in einer Vergleichsgruppe ab?

Grundlegende Schlüsselkontrolle

Im Folgenden finden Sie eine (unvollständige) Auswahl an grundlegenden Empfehlungen:

- Die sieben wichtigsten Sicherheitsmaßnahmen (Cybersecurity Centre Belgium)[28]
- Top Ten (UK National Cyber Security Centre)[29]
- Essential eight (Australisches Zentrum für Cybersicherheit)[30]
- Die 42 wichtigsten Maßnahmen für ein gesundes Netz (FR ANSSI)[31]
- Die acht wichtigsten Sicherheitsmaßnahmen (NL Nationales Zentrum für Cybersicherheit)[32]

Diese Behörden dienen außerdem als Quelle für aktuelle Informationen über die Bedrohungslandschaft und die Entwicklung von Schwachstellen und Angriffsmethoden.

[28] https://cyberguide.ccb.belgium.be/en/take-security-measures-0
[29] https://www.ncsc.gov.uk/files/2021-10-steps-to-cyber-security-infographic.pdf
[30] https://www.cyber.gov.au/acsc/view-all-content/essential-eight
[31] https://www.ssi.gouv.fr/en/guide/40-essential-measures-for-a-healthy-network/
[32] https://www.ncsc.nl/onderwerpen/basismaatregelen

Anhang 2: Beispiele aus der Community

Sammeln von Inputs

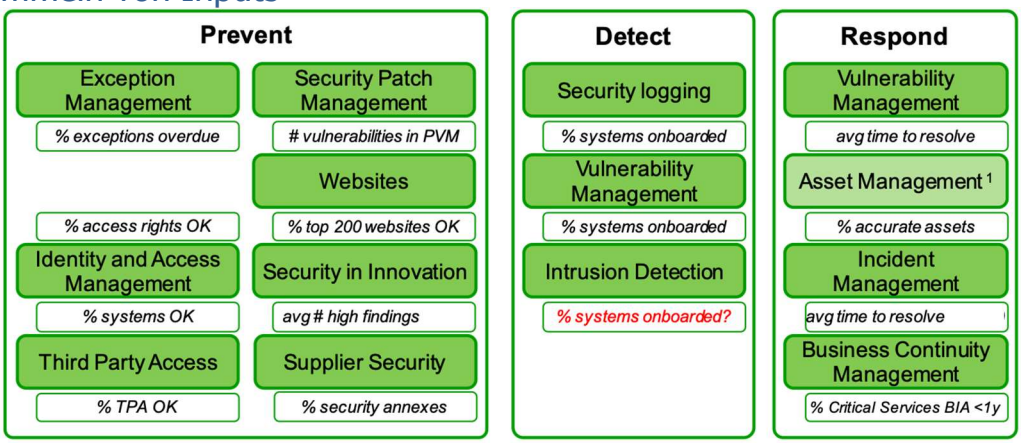


Abbildung 19 Beispiel für ereigniszentrierte Metriken

Incident Timeline	Applicability Level	Description
Time of First Activity	Recommended for significant incidents	This is the earliest event in a confirmed or potential chain of events, that caused the incident.
Time of Detection	All incidents	The time that a control (e.g. telemetry, technology) or another detection mechanism (e.g. a human) recognizes that something has occurred.
Time of Containment	All incidents that require Containment	Time of Containment is the point in time at which the incident can no longer spread nor do damage.
Time of Remediation	All incidents that require Remediation	Time of Remediation is the point in time at which an affected target asset is returned to its pre-incident state or removed from the environment permanently.

Abbildung 20 Empfohlene Timing-Metriken. Quelle: FIRST Metrics SIG.

Function	Category	Subcategory	Subcategory Risk	Sub Cat Score	Subcategory Composite Risk Score
	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 business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	Critical	6	30
		ID.AM-2: Software platforms and applications within the organization are inventoried	Weighted Medium	4	
		ID.AM-3: Organizational communication and data flows are mapped	Weighted Medium	4	
		ID.AM-4: External information systems are catalogued	Critical	6	
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Critical	6	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Weighted Medium	4	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	Weighted Low	2	
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Low	1	
		ID.BE-3: Priorities for organizational mission, objectives			

Abbildung 21 Ein Beispiel für die Umsetzung von Metriken in Verbindung mit der NIST CSF

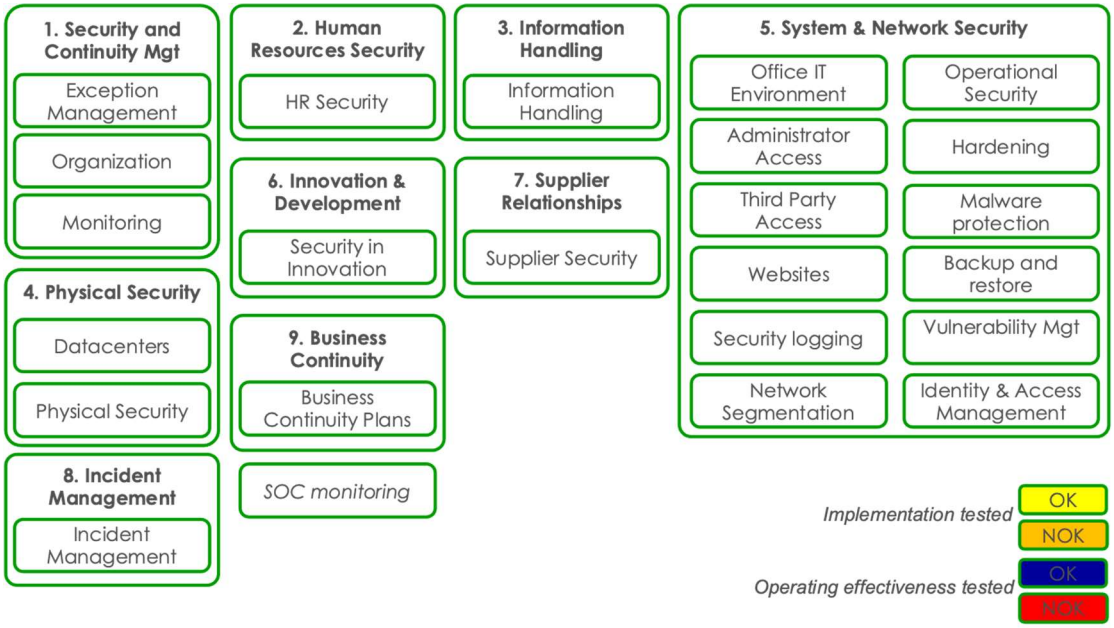


Abbildung 22 Beispiel für Metriken aus Tests

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Spearphishing Attachment	Command-Line Interface	Registry Run Keys / Startup Folder	Scheduled Task	Obfuscated Files or Information	Credential Dumping	System Network Configuration Discovery	Remote Desktop Protocol	Input Capture	Remote File Copy	Data Compressed	Data Encrypted for Impact
Valid Accounts	Scripting	Scheduled Task	Valid Accounts	Scripting	Input Capture	Process Discovery	Remote File Copy	Data from Local System	Commonly Used Port	Data Encrypted	Disk Structure Wipe
Drive-by Compromise	PowerShell	Valid Accounts	Process Injection	Valid Accounts	Brute Force	Account Discovery	Pass the Ticket	Data Staged	Standard Application Layer Protocol	Data Transfer Size Limits	Resource Hijacking
External Remote Services	Scheduled Task	New Service	New Service	Code Signing	Credentials in Files	File and Directory Discovery	Remote Services	Email Collection	Connection Proxy	Exfiltration Over Command and Control Channel	System Shutdown/Reboot
Spearphishing Link	Exploitation for Client Execution	External Remote Services	Accessibility Features	Deobfuscate/Decode Files or Information	Credentials from Web Browsers	Network Service Scanning	Windows Admin Shares	Audio Capture	Web Service	Exfiltration Over Alternative Protocol	
Exploit Public-Facing Application	User Execution	Create Account	Bypass User Account Control	File Deletion	Network Sniffing	Remote System Discovery	Windows Remote Management	Automated Collection	Custom Command and Control Protocol		
Supply Chain Compromise	Windows Management Instrumentation	Redundant Access	Web Shell	Masquerading	Account Manipulation	System Information Discovery	Component Object Model and Distributed COM	Data from Information Repositories	Multi-Stage Channels		
Trusted Relationship	Dynamic Data Exchange	Web Shell	Exploitation for Privilege Escalation	Process Injection		System Network Connections Discovery	Exploitation of Remote Services	Video Capture	Standard Non-Application Layer Protocol		
	Rundll32	Accessibility Features	DLL Search Order Hijacking	Connection Proxy		System Owner/User Discovery	Pass the Hash	Screen Capture	Uncommonly Used Port		
	Service Execution	Bootkit	Application Shimming	Redundant Access		Network Share Discovery		Data from Network Shared Drive	Fallback Channels		
	Graphical User Interface	Component Firmware		Rundll32		Permission Groups Discovery			Multi-hop Proxy		
	Mshta	BITS Jobs		Software Packing		Security Software Discovery			Data Obfuscation		
	Regsvr32	Modify Existing Service		Web Service		System Service Discovery			Domain Fronting		
	Execution through API	DLL Search Order Hijacking		Bypass User Account Control		Virtualization/Sandbox Evasion			Data Encoding		
	Component Object Model and Distributed COM	Shortcut Modification		DLL Side-Loading		Query Registry			Domain Generation Algorithms		
	Windows Remote Management	Windows Management Instrumentation Event Subscription		DLL Search Order Hijacking		Network Sniffing			Standard Cryptographic Protocol		
	CMSTP	Winlogon Helper DLL		Hidden Files and Directories		Peripheral Device Discovery					
	Compiled HTML File	Account Manipulation		Hidden Window							
		Application Shimming		Indicator Removal from Tools							
		Hidden Files and Directories		Indicator Removal on Host							
				Modify Registry							
				Mshta							
				Network Share Connection Removal							
				Process Hollowing							
				Regsvr32							
				Rootkit							
				Template Injection							
				Virtualization/Sandbox Evasion							
				Binary Padding							
				BITS Jobs							
				Disabling Security Tools							
				Execution Guardrails							
				Compiled HTML File							
				Component Firmware							
				CMSTP							
				Clear Command History							
				Compile After Delivery							

Abbildung 23 Beispiel für die Verwendung einer Heatmap zur Darstellung der Abdeckung von TTPs

Transformieren

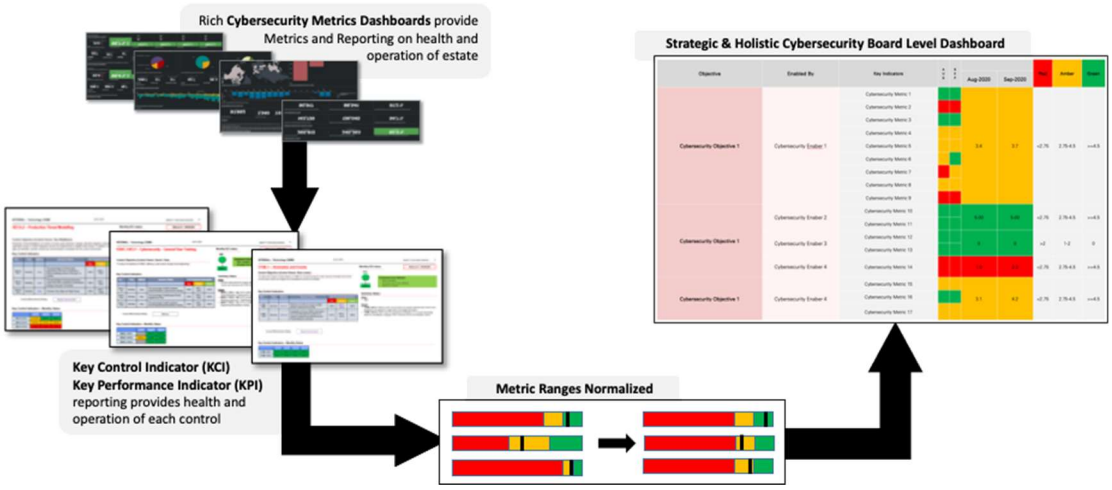


Abbildung 24 Beispiel für eine Normierung

Calculate Potential Harm Of Security Incidents for each security incident by two factors:

Likelihood:

How often would this vulnerability be exploited?

Potential Loss:

What would each exploit cost the company?

PHOSI = Likelihood x Potential Loss

Abbildung 25 Beispiel für die Monetarisierung

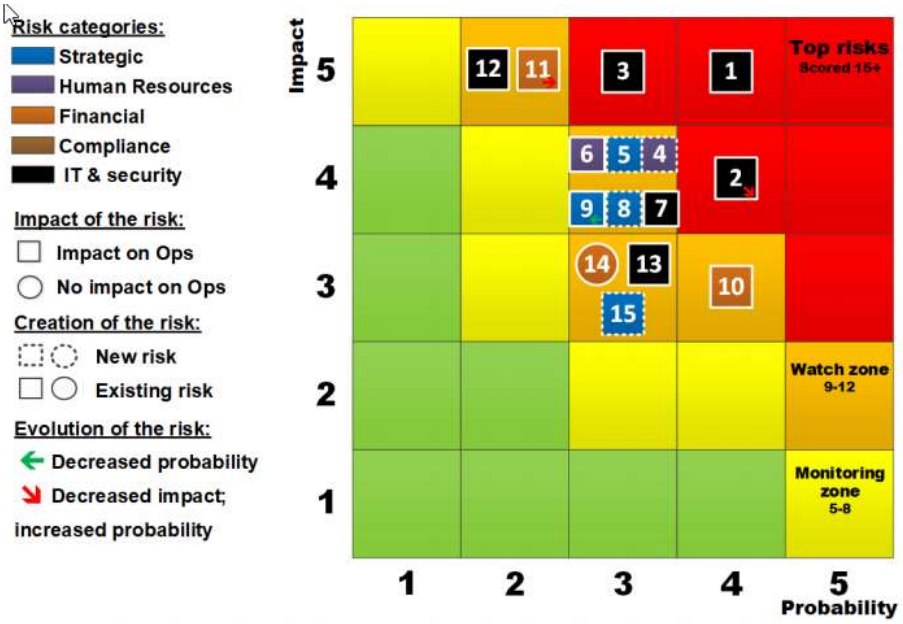
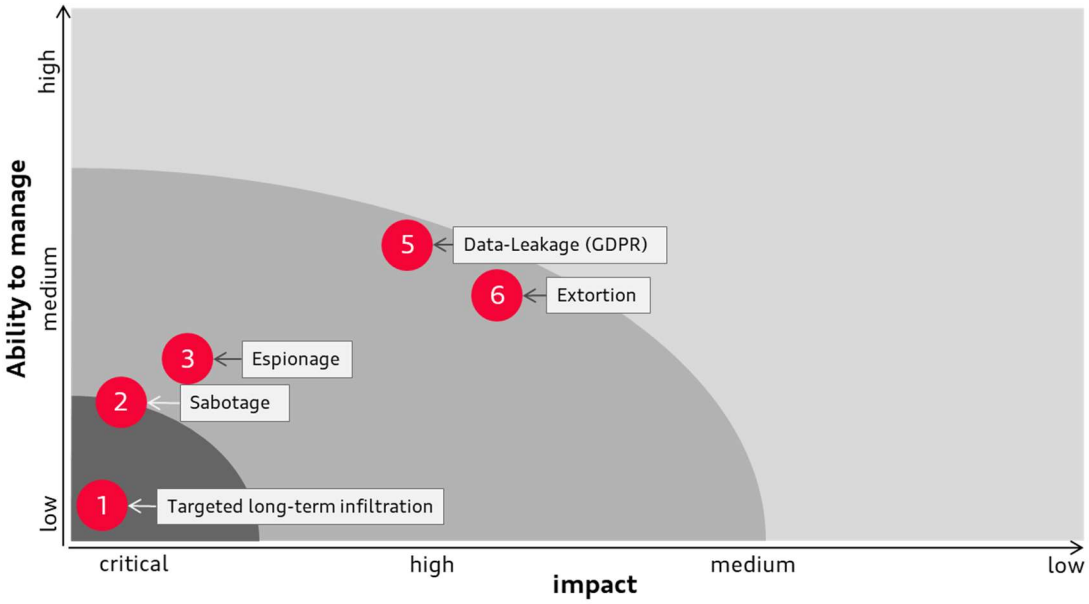


Abbildung 26 Beispiel für die Zuordnung zum Risiko

Meldung von Cyberrisiken



Manufacturing industry or geographically close

When?	What?	Category	Group
Q1.2021	Hackers exploit IT tool Z to establish persistence	1	Unknown
Q4 2020	Ransomware attack at enterprise X	2 6	Cyber-Crime
Q4 2020	Enterprise Y hit by ransomware, data leaked	2 6	Cyber-Crime

Abbildung 27 Beispiel für die Berichterstattung über die Bedrohungslandschaft

When	Type	What?	Status	Group
4/2020	3	Spear phishing campaign with malicious Excel attachment.	Closed	APTX

Abbildung 28 Beispiel für die Meldung von Vorfällen

Group	Motive	Trend
Adversary 1	Adversary known to steal intellectual property in high tech industry.	↗
Adversary 2	Adversary known to steal intellectual property in our sector.	→
Targeted Cyber-Crime	Ransomware actor increasingly prevalent and sophisticated	↑

Abbildung 29 Beispiel für die Verfolgung eines auffälligen Gegners

CERT-EU

TLP:WHITE

Threat Landscape Report 2021 Q3 - Executive Summary

Direct Threats to EU Institutions, Bodies, and Agencies

INCIDENTS

4 significant incidents affected EUIBAs this quarter.
In 3 cases the attack started with a compromise of a publicly accessible server (Oracle WebLogic, Microsoft Exchange).

In the other case, attackers obtained credentials via a phishing campaign.

In at least 3 significant incidents, threat actors successfully exfiltrated data.

Since the beginning of 2021, CERT-EU has already recorded 15 significant incidents, compared to 13 during the whole of 2020 and 8 in 2019.

THREATS

CERT-EU released 26 threat alerts (compared to 20 during Q1 and 22 in Q2).
The top 5 reasons for threat alerts were:

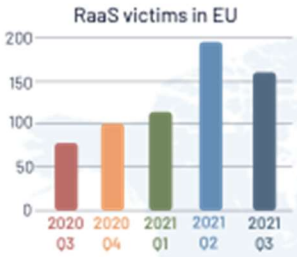
- Active exploitation of zero-days or n-days: Microsoft Exchange, VPNs, etc.
- Recent activity or new tools used by top threat actors
- Sharing actionable data related to TTPs used in significant incidents
- Spear-phishing campaigns directly affecting EUIBAs or sectors of interest
- Active use of commercial mobile spyware

Top threat actors: CERT-EU currently tracks 13 top threat actors. The level of exposure of EUIBAs has been high for 4 of them: two alleged Russian threat actors, one alleged Chinese, and one allegedly of North Korean origin.

Social media: The most frequently used social media network for impersonation of EU staff or the digital identities of EUIBAs has been Instagram, followed very closely by Facebook and at a distance by Twitter.

Malware and tools: The three most observed pieces of malware or malicious tools to which EUIBAs have been exposed were Cobalt Strike, Mimikatz, and Dridex. However, no infections have been confirmed.

Threats in Europe



Ransomware

A supply chain attack conducted by REvil against Kaseya VSA, software used by many MSPs, had a major impact on several organisations including in Europe, causing significant disruptions.

Taking into consideration the first 9 months of 2021, the average number of ransomware victims per month increased by 129% in 2021, compared to last year.

Nation-state activity

The EU has acknowledged and condemned Russian "Ghostwriter" cyberespionage / information operation activity against EU member states. The Russian APT29 threat actor targeted European governments with a zero-day exploit earlier in 2021. The EU, the UK, and the US attributed the Hafnium ProxyLogon attacks to China and are calling for an immediate stop to such adversarial activities. France reported a significant cyberespionage campaign by the Chinese Zirconium (aka APT31) threat actor. The NSO group and its Pegasus spyware have been used in several espionage cases against politicians and journalists.

Hacktivism

Belarussian hacktivists continue hack-and-leak operations against the Minsk regime.

Threats in the World

China: China is establishing full control over all domestic knowledge of software vulnerabilities. As always, China is active on social media, working to amplify pro-Chinese messages.

Russia: Political opposition and anti-corruption entities in Russia fall victim to DDoS attacks and data leaks. Stricter internet controls and censorship established before the September parliamentary election remain in place after the election. Proposed legislation prohibits foreign companies from processing biometric data of Russian citizens.

Iran: Iranian governmental websites were taken offline after a "cyber disruption".

North Korea: A North Korean cyber threat actor compromised a major South Korean major producer of combat ships & submarines.

CERT-EU, CERT for the EU Institutions, Bodies, and Agencies https://cert.europa.eu - services@cert.europa.eu

Abbildung 30 Beispiel für Metriken und Beschreibungen, Quelle: CERT-EU

Anhang 3: Musterbericht

Entwicklung der Bedrohungslandschaft

Who?	Group / Malware?	Why?	Trend
Adversary 1	APTX	Adversary known to steal intellectual property in high tech industry.	↗
Adversary 2	APTY	Adversary known to steal intellectual property in our sector.	→
Targeted Cyber-Crime	FIN11 (TA505)	Public and corporate IT-infrastructure is a growing market for ransomware	↑

Relevante Vorfälle und Bedrohungsentwicklungen

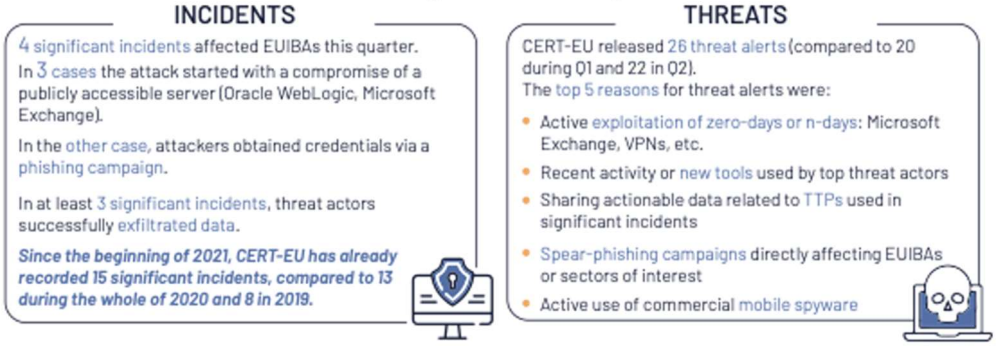
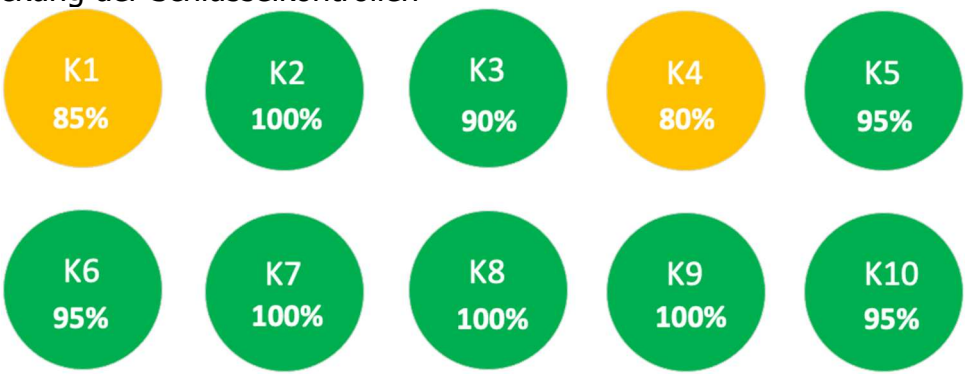
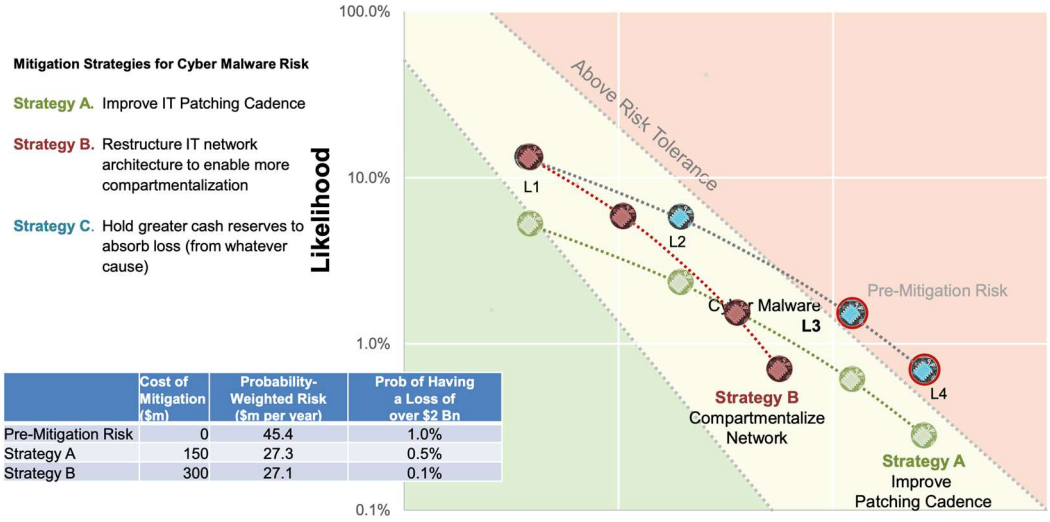


Abbildung 31 Quelle: CERT-EU

Abdeckung der Schlüsselkontrollen



Auswirkungen zusätzlicher Maßnahmen zur Minderung des Cyberrisikos



	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%

Abbildung 32 Quelle: Zentrum für Risikostudien, Universität von Cambridge