Berichterstattung über Cyber-Risiken an Vorstände

Ausgabe für Vorstände

Autoren
Freddy Dezeure
George Webster
Lokke Moerel

Rezensenten
Alan Kessler
Jamie Hutchinson

Datum: 14. März 2022
Version: Endgültige Fassung

Zweck

Dieses Papier gibt einen Überblick über den empfohlenen Ansatz für Vorstände im Umgang mit Cyber-Risiken und über gute Ausgangspunkte für Cyber-Metriken im Vorstand. Es ergänzt ein Papier, das sich an Chief Information Security Officers (CISOs) richtet, wie sie Cyber-Risiken am besten kontrollieren, messen und ihren Vorständen berichten können, und sollte in Verbindung mit diesem Papier gelesen werden.

Die meisten Vorstände sind nicht für das Cyber-Risiko sensibilisiert

Vorstände sind gesetzlich verpflichtet, eine angemessene Risikoüberwachung zu gewährleisten. Cyber-Risiken stellen mittlerweile ein kritisches, potenziell wesentliches Geschäftsrisiko dar. Die meisten Vorstände sind jedoch schlecht für den Umgang mit Cyberrisiken gerüstet. Sie betrachten Cyberrisiken als zu technisch, genehmigen lediglich Ressourcen und delegieren das Risiko.

Für traditionelle Geschäftsrisiken gibt es eine etablierte Praxis, wie Anzeichen und eine akzeptierte Verteilung der Verantwortung/Delegation zu melden sind. Für Cyberrisiken gibt es derzeit keine etablierte Praxis. CISOs haben Mühe, die Wirksamkeit ihrer Cybersicherheitsprogramme zu messen und hinreichend zu gewährleisten, dass das verbleibende Cyberrisiko unter der Risikobereitschaft des Unternehmens bleibt. Viele CISOs sprechen nicht die „Vorstandssprache" und werden nicht zur Berichterstattung aufgefordert.

In den Ausnahmefällen, in denen eine Berichterstattung über Cyber-Risiken an den Vorstand erfolgt, wird eine Vielzahl von Methoden, Instrumenten und Verfahren eingesetzt. Häufig geht es bei der Berichterstattung um den Fortschritt bei der Umsetzung von Cybersicherheitsmaßnahmen (Messung der *Anstrengungen*, oft Berichterstattung im grünen Bereich) und nicht um die *Risikominderung*.

Es geht um das Risiko

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 Risikobewertungen erleichtert und objektiviert. Im Cyber-Bereich verwenden wir ein Modell, bei dem sich das Risiko aus drei Faktoren zusammensetzt: **Bedrohung**, **Schwachstelle** und **Auswirkungen**.

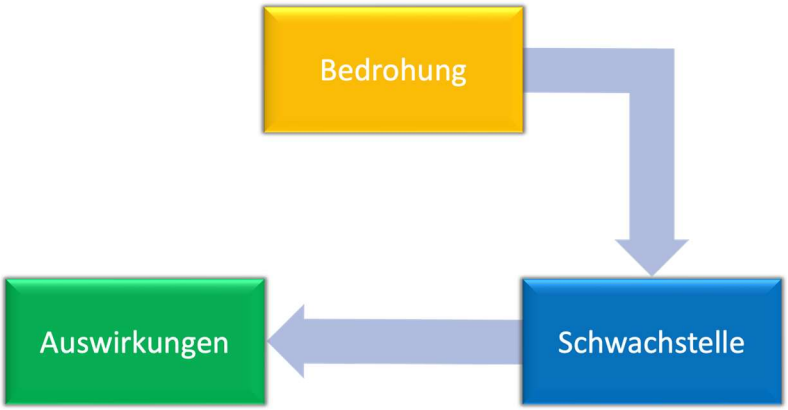


Abbildung 1 Risiko als Kombination aus Bedrohung, Schwachstelle und Auswirkungen

Die Bedrohung liegt meist außerhalb unserer Organisation und ist eng mit den Gegnern verbunden, die unserer Organisation schaden könnten. Die Identifizierung unserer **wichtigsten Gegner** und ihrer Motive ist wichtig für die Festlegung von Prioritäten bei unseren Abwehrmaßnahmen. Wir können aktuelle Bedrohungen beobachten und versuchen, zukünftige Bedrohungen vorherzusagen.

Der zweite Faktor ist die **Schwachstelle**, auf die wir am meisten Einfluss nehmen können, indem wir Kontrollen und Abhilfemaßnahmen entwerfen und umsetzen. 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, das Durchsickern personenbezogener Daten, die Unterbrechung von Diensten, den persönlichen Schaden und die Schädigung der Marke. Die Auswirkungen sind eng mit den Vermögenswerten verbunden. Die Identifizierung unserer **wichtigsten Vermögenswerte** ist wichtig für die Festlegung von Prioritäten.

Empfohlener Ansatz für Vorstände beim Umgang mit Cyberrisiken

1. Cyber-Bewusstsein entwickeln und angemessene Sicherheit erlangen

Verlangen Sie eine regelmäßige Berichterstattung und nicht nur im Falle eines Vorfalls. Fördern Sie eine ernsthafte Berichterstattung und nicht nur „Entwarnung". Bestehen Sie auf interner Abstimmung und klaren Kommunikationskanälen, wobei der CISO eine zentrale Rolle spielen sollte, um eine professionelle und unabhängige Sicht auf das Cyberrisiko zu gewährleisten[1] .

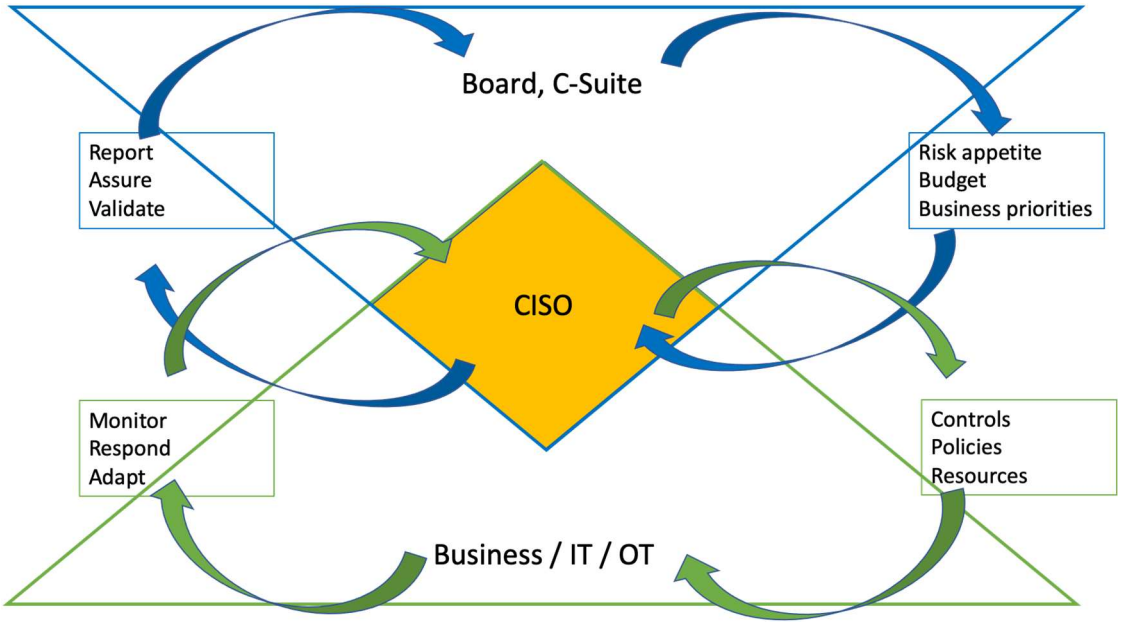


Abbildung 2 Informationsflüsse und die Rolle des CISO als Koordinator.

[1] Informationsflüsse, inspiriert von NIST Cyber Security Framework https://www.nist.gov/cyberframework

Die Berichterstattung über Cyber-Risiken sollte dazu dienen, dem Vorstand (erneut) zu versichern, dass das Risiko heute und morgen 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?

Die gemeldeten Metriken könnten mit Informationen über wichtige Vorfälle innerhalb und außerhalb des Unternehmens, über Bedrohungen und rechtliche Entwicklungen kombiniert werden. Der CISO sollte alle Entwicklungen melden, die die Situation wesentlich zum Besseren oder Schlechteren verändern, und infolgedessen entsprechende Maßnahmen und Ressourcen vorschlagen.

Ein Musterbericht zur Veranschaulichung einer möglichen Berichtsstruktur mit Beispielzahlen ist im Anhang beigefügt.

2. Stellen Sie die richtigen Fragen zur Situation

Fragen, die Vorstände ihrem CISO stellen sollten, stehen in engem Zusammenhang mit den Risikofaktoren.

- Verfügen wir über ein Inventar der wichtigsten Vermögenswerte?
- Welche Arten von Gegnern haben es auf uns abgesehen und warum?
- Welche sind unsere wichtigsten Kontrollen und welchen Status haben sie?
- Wo sind die Lücken und wie wollen wir sie schließen?
- Verfügen wir über einen Plan für die Reaktion auf Zwischenfälle / Geschäftskontinuität / Widerstandsfähigkeit?
- Welches Risiko besteht?
- Wie schneiden wir im Vergleich zu unseren Mitbewerbern und unserem Sektor ab?

3. Kontrollieren Sie Ihre Risiken

Rahmenwerke für Cybersicherheit sind ein Instrument zur kohärenten Verwaltung von Cybersicherheitsrisiken und zur Umsetzung einer Cybersicherheitsstrategie für Unternehmen. Weit verbreitete Rahmenwerke sind ISO/IEC 27001[2] und NIST's Cyber Security Framework.[3] Es spielt keine große Rolle, für welches Rahmenwerk sich eine Organisation entscheidet, da es Entsprechungen zwischen ihnen gibt. Für Vorstände ist es jedoch wichtig, sicherzustellen, dass es eine vollständige interne Abstimmung (zwischen CISO, IT/OT und Risikomanagement) darüber gibt, welches Framework von der Organisation verwendet wird.

Rahmenwerke enthalten in der Regel Hunderte von Kontrollen, über die auf Vorstandsebene nicht berichtet werden kann. Daher müssen die Schlüsselkontrollen ermittelt werden. Ein guter Ausgangspunkt sind die von den verschiedenen nationalen Cybersicherheitsbehörden herausgegebenen Leitlinien. Es gibt ein hohes Maß an Überschneidungen zwischen diesen

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

verschiedenen grundlegenden Anleitungen, die einen ausgezeichneten, knappen und praktischen Ausgangspunkt bieten. Nachstehend sind einige der wichtigsten Kontrollen aufgeführt, 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).

Die Abschwächung jeder Kontrolle könnte durch einen „Coverage Score" gemessen und gemeldet werden, der die Einführung, den Betrieb und die Wirksamkeit einer Kontrolle kombiniert.

Anhang: 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	State sponsored actor known targeting critical infrastructure	↗
Adversary 3	FINX	Ransomware actor increasingly prevalent and sophisticated	↗

Relevante Vorfälle und Bedrohungsentwicklungen

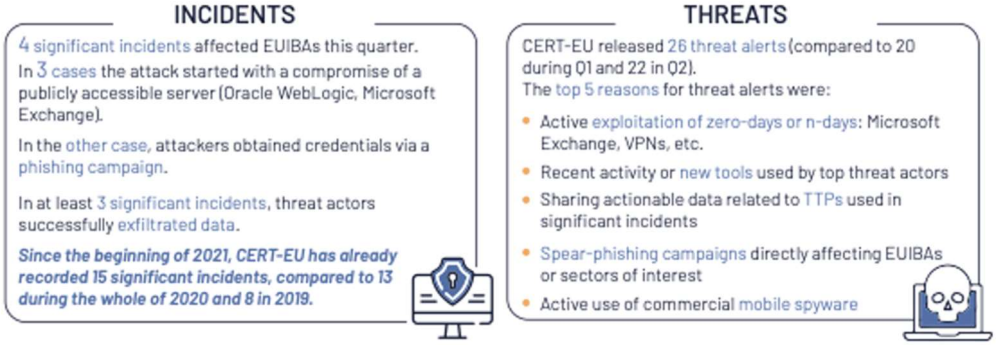
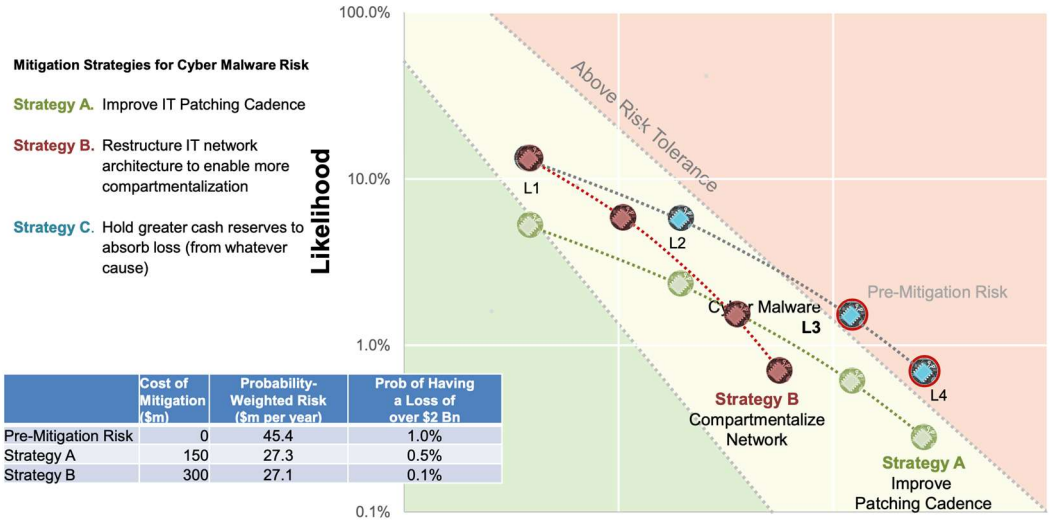


Abbildung 3 Quelle: CERT-EU

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 4 Quelle: Zentrum für Risikostudien, Universität von Cambridge