10/24

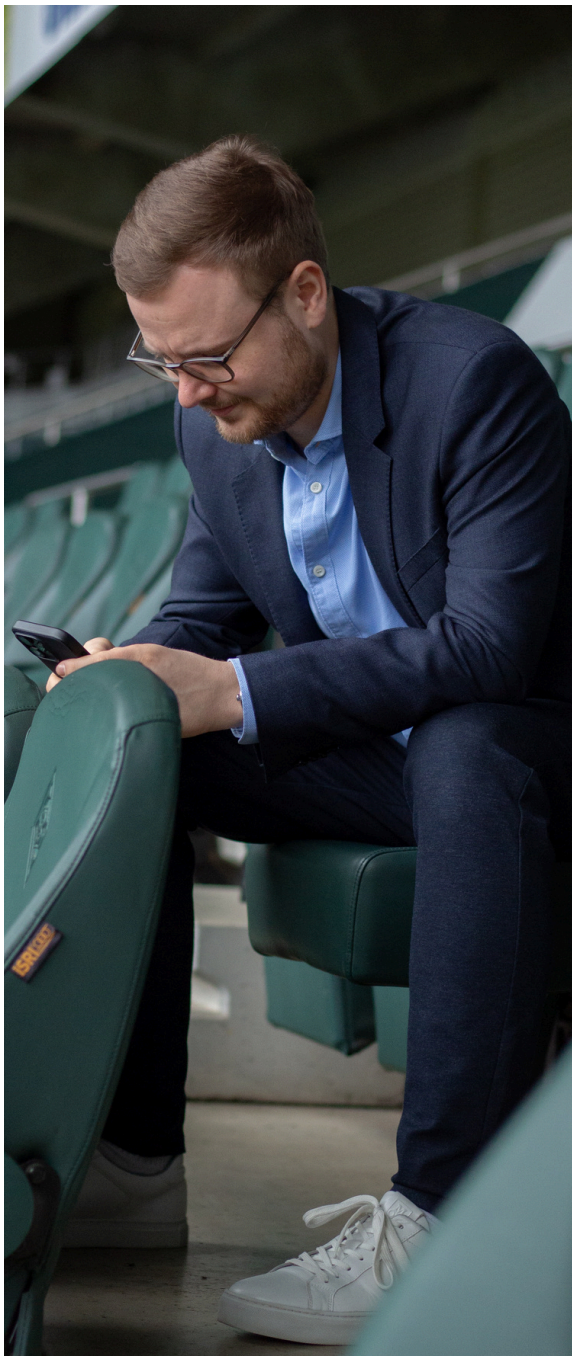
secure mag

CISO Strategien für Cybersecurity

Cyber-Resilienz als Wettbewerbsvorteil

Einleitung

Du bist CISO/CIO und trägst die Verantwortung für die IT-Sicherheit in deinem Unternehmen. Von der Geschäftsführung bist du dazu berufen worden, eine Cybersecurity-Strategie zu entwickeln, um die Cyber-Resilienz sukzessive zu steigern.



Dann kennst du vielleicht schon die ein oder andere Herausforderung:

- Du hast noch nie eine Cybersecurity-Strategie erstellt
- Du hast kein dediziertes Budget oder Planstellen zur Verfügung
- Du hast keine externen Partner, die dich unterstützen
- Du hast ein Problem damit, die Geschäftsführung für deine Themen zu sensibilisieren
- Die Mitarbeitenden unterstützen die Umsetzung der Security-Maßnahmen nicht ausreichend

Wenn du dich von diesen Herausforderungen angesprochen fühlst, dann findest du im Folgenden einige hilfreiche Lösungsvorschläge.

1. So konzipierst du eine Cybersecurity-Strategie

Manche haben eine, viele wollen eine und dabei brauchen alle eine. Denn eine solide Strategie bildet die Basis für die Planung von Maßnahmen zur Erhöhung der Cyber-Resilienz. Doch wie fange ich das am besten an?

Zuerst muss ich verstehen: Welches sind die kritischsten Geschäftsprozesse? Hier macht es Sinn sich an bestehenden Dokumenten zu orientieren. Im besten Fall liegt schon eine Business Impact Analyse vor, ansonsten hilft auch ein Interview mit der Geschäftsführung oder anderen relevanten Personen.

Denn alle Prozesse maximal zu schützen ist wirtschaftlich kaum möglich und auch nicht notwendig. Deshalb sollte der Fokus auf den kritischen Prozessen liegen. Das sind in der Regel alle Prozesse entlang der Wertschöpfungskette. Die Annäherung erfolgt damit aus der Business-Perspektive.

Wenn ich das verstanden habe, kann ich im nächsten Schritt die IT-Assets den Prozessen zuordnen und damit kritische IT-Assets definieren. Dies erfolgt effizient über ein Asset Management System.

Durch die Zuweisung der kritischen Geschäftsprozesse zu den IT-Assets kann ich jetzt sehr einfach Abhängigkeiten identifizieren. Es ermöglicht mir auch zielgerichtete Simulationen wie z. B:

- Was passiert, wenn dieses Asset nicht mehr verfügbar ist?
- Was wäre das Risiko, wenn die Informationen von diesem Asset entwendet werden?

Ich beginne den Risikomanagement-Prozess. Kurz gesagt: Welche Angriffe würden mir besonders weh tun und womit könnte ich leben?

Alle Risiken, die mir besonders weh tun möchte ich am liebsten mit entsprechenden Maßnahmen mitigieren. Diese Maßnahmen sollten den 3 Kernzielen der IT-Sicherheit zugeordnet werden:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Eine Strategie begleitet ein Unternehmen im besten Fall über mehrere Jahre. Deshalb plane ich auf der Basis eine entsprechende Roadmap mit klarer Priorisierung der Maßnahmen. Für jede Maßnahme überlege ich mir, welche Ressourcen für die Umsetzung notwendig sind. Damit bin ich in der Lage ein grobes Budget und auch möglichen Zuwachs für Personal abzuleiten.

Im Ergebnis habe ich nun eine Cybersecurity-Strategie, eine Roadmap für die Umsetzung und ein Verständnis dafür, wie viel zusätzliches Budget und Personal ich dafür benötige.

2. Budget und Planstellen durch Cybersecurity als Wettbewerbsvorteil

Durch die Erstellung der Cybersecurity-Roadmap habe ich nun ein grobes Verständnis, wie viele Ressourcen benötigt werden. Jetzt braucht es noch das nötige Budget zur Umsetzung. Doch wie mache ich das am besten?

Wenn ich etwas haben möchte, dann muss ich auch etwas geben. Es ist wenig zielführend nur zu fordern. Ich muss also verstehen, was sind die Ziele meiner Geschäftsführung?

In der Regel ist die Geschäftsführung dafür verantwortlich, ein profitables und wachsendes Geschäft aufzubauen. Investitionen in IT-Sicherheit zeigen jedoch oft zunächst keinen direkten Profit, sondern kosten Geld und verlangsamen Prozesse, um negative Ereignisse zu verhindern. Daher ist es wichtig, der Geschäftsführung klarzumachen, welche Vorteile die Genehmigung der Budgets bringt.

Beispielsweise:

- Wir stellen sicher, dass unsere Produktion nicht von einem Betriebsausfall betroffen wird
- Wir stellen sicher, dass die streng geheime Rezeptur unseres Kassenschlagers auch streng geheim bleibt
- Wir stellen sicher, dass wir weiter liefern können, während unsere Wettbewerber gehackt wurden
- Wir stellen sicher, dass das in uns gesetzte Vertrauen unserer Geschäftspartner gerechtfertigt ist

Die Message muss sein: Wir machen IT-Sicherheit nicht zum Selbstzweck, sondern zum Schutz unserer digitalen Geschäftsprozesse und damit zu einem echten Wettbewerbsvorteil. Je genauer die Use-Cases auf das eigene Unternehmen angepasst sind, umso besser ist dies für die Geschäftsführung nachvollziehbar. Auf generalistische Drohungen sollte besser vermieden werden.

"Wenn wir jetzt nicht viel Geld in die IT-Sicherheit investieren, ergeht es uns wie der Firma xyz". Solche Hiobsbotschaften hört die Geschäftsführung oft und schreckt eher ab, sich mit dem Thema zu beschäftigen.

Nachdem ich nun der Geschäftsführung gezeigt habe, wie die Erhöhung der Cybersicherheit zu den Unternehmenszielen beiträgt, beginne ich mit der Argumentation bzgl. des Budgets.

Hierbei muss ich im Wesentlichen zwei Dinge beachten:

- Benchmarks und Referenzen
- Optionen schaffen

Wenn ich bei meiner Geschäftsführung nun 10 Planstellen und 10 Millionen € einfordere, dann muss ich gleichzeitig auch Referenzen dafür mitbringen. Natürlich kann ich alles so detailliert wie möglich ausarbeiten und das hilft mir natürlich, meine Forderungen zu untermauern, aber relativ schnell werde ich die Frage hören: "Wie viel Budget ist üblich? Was geben andere Unternehmen so aus".

Natürlich können wir jetzt keine empirische Studie durchführen, aber wir können mit allgemeinen Empfehlungen arbeiten. Zum Beispiel empfiehlt das BSI, 20 % des IT-Budgets für IT-Sicherheit vorzusehen. Ich gehe also von beiden Seiten heran, einmal liefere ich meine erarbeiteten Werte und untermauere diese zusätzlich mit der Empfehlung einer in Deutschland allgemein anerkannten Behörde..

Eine Geschäftsführung ist dazu da, Entscheidungen zu treffen, aber Entscheidungen können nur getroffen werden, wenn es eine Auswahl gibt. Im besten Fall erstellen wir also drei schlüssige Pläne und dann sehr genaue Argumentationsstränge, welche Wahl die beste wäre.

Um es einfach zu halten, arbeiten wir z. B. mit T-Shirt-Größen und bieten ein Paket S, M und L an. Das Paket S beinhaltet dann die Basisabsicherung, das Paket M alle Maßnahmen, die ich für den Schutz der kritischen Geschäftsprozesse für angemessen halte und das Paket L noch etwas mehr.

Kleiner Tipp vorweg: Die meisten Menschen entscheiden sich für M.

3. Die Evaluierung externer Dienstleister

Personalkosten sind in vielen Unternehmen die höchsten Kostentreiber und deswegen achtet die Geschäftsführung oftmals sehr genau auf diese. Daher werden auch oft eher Investitionen in Software genehmigt oder externe Dienstleister beauftragt als Investitionen in die IT-Sicherheit..

So bezahle ich beispielsweise Dienstleister nur, wenn ich eine Dienstleistung in Anspruch nehme. Das Personal hingegen wird das ganze Jahr über bezahlt. Außerdem existiert in der IT-Branche und insbesondere der IT-Security-Branche ein Fachkräftemangel. Jeder sucht aktuell Experten und es ist unheimlich schwer, diese zu finden und zu halten.

Das heißt vermutlich werden mir nicht so viele Planstellen freigegeben wie ich mir wünsche und diese sind auch noch schwer zu besetzen. Ein valider Lösungsansatz ist es, auf Managed Services und externe Beratungsleistungen zu setzen. Nicht umsonst boomen diese Märkte aktuell wie lange nicht.

Der Nachteil des boomenden Marktes ist, dass jeder mitverdienen will. Dadurch gibt es viel Intransparenz bei den Angeboten und nicht selten kann ein Unternehmen nicht halten, was es verspricht.

Ich brauche also Zeit bei der Evaluierung. In der Evaluierungsphase sollten ein paar grundlegende Fragestellungen geklärt werden:

- In welchen Bereichen möchte ich auf externe Unterstützung setzen und in welchen nicht?
- Wie ist meine Erwartungshaltung an den Dienstleister?
- Welche Anforderungen habe ich gegebenenfalls im Speziellen an einzelne Produkte oder Services?

Wenn ich keine klare Erwartungshaltung habe, ist es schwierig, diese zu erfüllen. Die Frage ist, wie sieht "Mein" optimaler Dienstleister aus. Einen Überblick der Anbieter am Markt ermöglichen z. B. gängige Marktforschungsinstitute wie ISG-Provider Lens, Gartner oder Forrester. Zusätzlich empfiehlt sich eine Bewertungsmatrix, die alle wichtigen Kriterien beinhaltet und mir einen Vergleich der Dienstleister ermöglicht.

4. So verschaffst du dir Gehör im Management

Du hast eine umfassende Cybersecurity-Strategie entwickelt und die Roadmap detailliert ausgearbeitet, aber dennoch erhältst du nicht die Reaktion, die du erwartet hast. Warum ist das oftmals so?

Um das zu erklären, hilft es, sich in die Rolle des Ansprechpartners zu versetzen. Die Geschäftsführung ist am Ende für alles im Business verantwortlich. Vom Marketing über die Finanzen bis hin zum Personal.

Jeden Tag kommt das Management mit neuen Vorschlägen um die Ecke. "Wir sollten diese Maßnahmen umsetzen, das wird alle Probleme lösen. Wir brauchen nur etwas Geld und Zeit von dir". Die Tage sind vollgepackt mit Meeting-Marathons in denen Entscheidungen gefällt werden müssen, und die Tragweite der Entscheidungen sind relativ groß.

Die typische Geschäftsführung steht täglich unter Druck, die richtige Entscheidung zu treffen. Falsche Entscheidungen können Arbeitsplätze kosten, oder im Worst-Case die Existenz des Unternehmens. Wir müssen es der Geschäftsführung leicht machen, die richtigen Entscheidungen treffen zu können.

Das können wir entweder über einen jahrelangen positiven Track-Record machen, indem die Geschäftsführung gelernt hat, wenn du etwas vorschlägst, dann kann sie das blind unterschreiben oder dadurch, dass die Entscheidungs-vorlage zielgruppengerecht aufgebaut ist. Das heißt, ich muss es der Geschäftsführung leicht machen, eine Entscheidung zu fällen.

Hier ist weniger mehr. Sie muss auf einen Blick erkennen können, welche Chancen und Risiken habe ich, wenn ich mich für einen der aufgezeigten Wege entscheide. Das Ganze gerne visuell, kurz und prägnant aufgearbeitet. Dennoch muss ich genügend Material und Quellen in der Hinterhand halten, um Rückfragen Stand zu halten.

Die Geschäftsführung ist dafür bekannt, schnell und zielgerichtet unangenehme Fragen zu stellen. Darauf muss ich vorbereitet sein, denn komme ich ins Straucheln, kann das ganze Kartenhaus zusammenklappen.

Oftmals stelle ich mir dann selbst zur Vorbereitung des Termins die Frage "Welche unangenehmen Fragen könnten auf mich zukommen?". Denn es ist eine der Kernaufgaben der Geschäftsführung, die Konzepte zu hinterfragen.

5. Der Weg zu einer cyber-sensitiven Unternehmenskultur

Du hast das Management Buy-In und damit die Rückendeckung der Geschäftsführung erhalten und bist mit ausreichend Budget und Planstellen ausgestattet. Du willst jetzt richtig loslegen, aber das erste, was du hörst aus der Belegschaft ist:

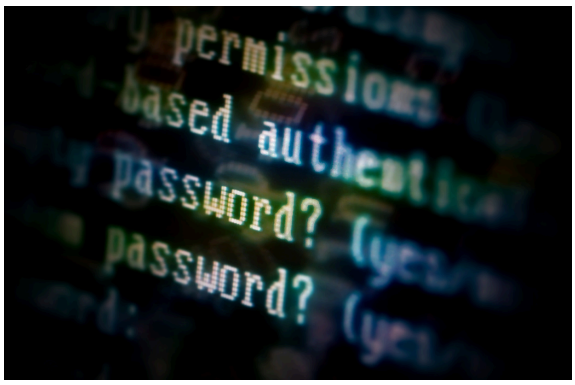
"Früher war alles besser, jetzt müssen wir uns jeden Tag mit dem Authenticator herumschlagen, um uns alle 4 Stunden einzuloggen. Das macht das keinen Spaß mehr. Wir müssen dringend mit der Geschäftsführung sprechen."

Damit dein Security Programm nicht ins Stocken kommt, ist es unfassbar wichtig, eine gesunde Change Kultur im Unternehmen zu etablieren. Durch die Einführung stärkerer IT-Sicherheits-richtlinien und -prozesse haben wir direkten Einfluss auf den Arbeitsalltag der Belegschaft.

Peter durfte 20 Jahre lang seinen USB-Stick in jeden Slot stecken und jetzt ist plötzlich Schluss damit oder aber der Bildschirm sperrt sich automatisch bei längerer Abwesenheit und jetzt muss er sich wieder neu einloggen. Tatsächlich führt jede Maßnahme zu erhöhten Aufwänden bei den Mitarbeitenden.

Auch hier ist es wieder wichtig, den Menschen verständlich zu machen "what's in for me". Daher empfiehlt es sich das Security Programm im Unternehmen zu kommunizieren, das Personal um Unterstützung zu bitten und zu präsentieren, was die Vorteile sind und welche Nachteile dadurch nicht eintreten.

Natürlich ist es lästig, wenn ich nun bei jedem Login den Authenticator benutzen muss, was mich vermutlich ca. 30 Sekunden am Tag kostet. Aber wie sieht die Alternative aus? Wie sieht es aus, wenn das Unternehmen einen existenzbedrohenden Ransomware-Angriff erleidet und in der Folge Abteilungen geschlossen werden und Arbeitskräfte den Job verlieren.



Aufklärung spielt hier eine essenzielle Rolle. Je besser die Menschen verstehen, warum diese Maßnahmen wichtig sind, desto größer ist die Akzeptanz. Kommunikation ist ein absolutes Schlüsselelement.

Key-Take-Aways:

- Eine klare Priorisierung der Maßnahmen ist unerlässlich
- Cybersecurity sollte als Wettbewerbsvorteil kommuniziert werden
- Transparente Kommunikation fördert die Akzeptanz in der Belegschaft
- Eine strukturierte Roadmap und effektives Risikomanagement sind entscheidend

Zusammenfassung

Als CISO/CIO trägst du die Verantwortung für die Cyber-Resilienz des Unternehmens. Dabei ist weniger dein technisches Know-how entscheidend, sondern vielmehr die Priorisierung der Maßnahmen.

Fokussiere dich auf die kritischen Geschäftsprozesse und ordne die IT-Assets entsprechend zu. Es ist wichtig, die Risiken zu identifizieren und eine klare Roadmap zu erstellen, um die erforderlichen Ressourcen und Budgets zu ermitteln.

Um die Geschäftsführung zu überzeugen, solltest du Cybersecurity als Wettbewerbsvorteil präsentieren und die geschäftlichen Vorteile klar kommunizieren. Eine transparente Kommunikation und das Verständnis für die Bedeutung von Sicherheitsmaßnahmen sind entscheidend, um die Akzeptanz in der Belegschaft zu fördern.

Weitere Informationen zum Thema:

Podcast-Folge:

Cybersecurity-Strategie:
CISOs zwischen Schutz und Managementanforderungen

suresecure gmbh
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.de