3. Prognose-, Chancen- und Risikobericht

3.1 Risikobericht

3.1.1 Risikomanagementziele und -methoden

Das Risikomanagement wird für den secunet-Konzern und für die secunet AG in gleicher Weise und parallel durchgeführt. Daher treffen die im folgenden dargestellte Funktion sowie die Beschreibung von Einzelrisiken und -chancen sowohl auf den secunet-Konzern als auch auf die secunet AG zu.

Das Risikomanagement findet bei secunet auf verschiedenen Ebenen statt: Risiken, denen mittels strategischer, mittel- bis langfristigen Maßnahmen begegnet wird, werden als Rahmenbedingungen der mittelfristigen strategischen Unternehmensplanung durch den Vorstand berücksichtigt. Risiken mit Blick auf die in der laufenden Jahresplanung festgelegten Ziele werden in einem dedizierten Risikoausschuss behandelt. Operative Risiken schließlich werden im Rahmen der täglichen operativen Routinen und Risikominimierungsmaßnahmen berücksichtigt und weitestgehend entsprechend reduziert bzw. ausgeschlossen.

Das Risikofrüherkennungs- und Risikomanagementsystem der secunet AG wird laufend weiterentwickelt und optimiert.

3.1.2 Strategisches Risikomanagement und strategische Risiken

Mittel- und langfristige Risiken für secunet werden im Rahmen der strategischen Planung berücksichtigt. Eine Erörterung dieser Rahmenbedingungen sowie der Konsequenzen auf die Strategie findet regelmäßig mit dem Aufsichtsrat statt, der diese Planung genehmigt und weiterverfolgt.

Zu den hier betrachteten Risiken gehören unter anderem die folgenden:

Als mittelfristiges Vertriebsrisiko ist der Risikofaktor Kundenstruktur zu sehen, der sich darin offenbart, dass secunet den Hauptanteil seines Geschäfts mit Behörden und Organisationen aus dem öffentlichen Sektor abwickelt. Der Verlust von Teilen der Nachfrage dieser Kundengruppe kann sich negativ auf Umsatz und Ergebnis auswirken. Dieses Risiko wird regelmäßig ausführlich diskutiert. IT-Investitionen und darunter vor allem die Investitionen in IT-Sicherheit gelten als besonders wichtig für die reibungslose Erfüllung staatlicher Aufgaben, zumal in einer immer stärker durch Informationstechnologie geprägten Welt. Daher wird das Risiko des Ausfalls staatlicher Nachfrage zwar laufend begutachtet, derzeit aber als vergleichsweise gering angesehen.

Um mittelfristig auf das eventuelle Risiko eines Nachfragerückgangs vonseiten der staatlichen Kunden besser reagieren zu können bzw. um den daraus entstehenden Umsatz- und Ergebnisrückgang zu reduzieren und zu kompensieren, wird secunet auch weiterhin intensiv den Ausbau seiner Aktivitäten bei der Zielgruppe der privaten Wirtschaft (Business Sector) vorantreiben.

Ein weiteres Risiko kann darin gesehen werden, dass ein großer Teil der Umsatzerlöse sich auf einige wenige öffentliche Bedarfsträger und Unternehmen konzentriert. Fällt einer dieser größeren Kunden auch nur kurzfristig aus und verschieben sich entsprechend erwartete Beauftragungen, kann zumindest die Erreichung von Jahreszielen für secunet gefährdet sein. Auch hier kann der Einsatz von Key Account Managern im Vertrieb zur Risikominderung hilfreich sein. Er ermöglicht über den engen Kontakt zum Kunden eine rechtzeitige Reaktion auf Veränderungen der Nachfrage.

Zudem wird es als Risiko für das weitere Wachstum von secunet angesehen, dass die Geschäftsergebnisse noch immer stark durch die Nachfrage aus dem nationalen Umfeld beeinflusst werden. Daher stehen auch weiterhin der Ausbau eines leistungsfähigen internationalen Vertriebs, die Erschließung neuer Märkte und die Gewinnung weiterer Kunden im Ausland mit im Fokus der Anstrengungen für die zukünftige Entwicklung der Gesellschaft. Eine strategische Maßnahme ist die Bündelung der internationalen Vertriebsaktivitäten in der eigens dafür gegründeten Gesellschaft.

Die auf dem deutschen Markt für IT-Sicherheit vorherrschenden guten geschäftlichen Rahmenbedingungen haben besonders in der jüngeren Vergangenheit neue Wettbewerber angezogen. Die damit verbundene, sich verändernde Wettbewerbsintensität wird von secunet fortlaufend beobachtet und evaluiert. Gegenwärtig sieht die Gesellschaft keine negativen Auswirkungen auf die Marktstellung von secunet.

3.1.3 Risikomanagement für das laufende Plan- und Geschäftsjahr

Das Management von Risiken mit Blick auf die in der laufenden Jahresplanung festgelegten Ziele wird bei secunet durch einen Risikoausschuss wahrgenommen. Diesem gehören die Mitglieder des Vorstands sowie der für Risikomanagement zuständige Bereichsleiter an. Der Risikoausschuss trifft sich zu regelmäßigen Sitzungen einmal im Quartal. Sämtliche Entwicklungen, die eine Gefahr für die Zielerreichung oder sogar den Fortbestand des Unternehmens darstellen könnten, werden vom Risikoausschuss intensiv analysiert, beobachtet und bewertet. Ziel ist es, möglichst frühzeitig Informationen über Risiken und die damit verbundenen finanziellen Auswirkungen zu erlangen, um geeignete Maßnahmen zu ergreifen. Gleichzeitig sollen auch die bestehenden Chancen mit dem dann einhergehenden Ergebnispotenzial erkannt und genutzt werden.

In Vorbereitung der Sitzungen des Risikoausschusses findet jeweils eine umfassende Risikoinventur in allen Bereichen des Unternehmens statt. Nach einem Bottom-up-Ansatz werden die Risiken identifiziert, aggregiert und nach ihrer Schadenhöhe und nach ihrer Eintrittswahrscheinlichkeit bewertet.

Die so erhobenen unternehmensspezifischen Risiken werden im Rahmen der Sitzungen des Risikoausschusses top down erörtert und validiert. Eine Saldierung der Wirkungen von Risiken und Chancen erfolgt nicht. Bei der Betrachtung der potenziellen Schadenwirkungen von Risiken wird auf eine Nettobetrachtung abgestellt, d.h. dass die Auswirkungen bereits getroffener Risikobegrenzungsmaßnahmen in die Bewertung eingerechnet werden. In Abhängigkeit des wahrscheinlichkeitsgewichteten Schadenwerts der Risiken (Risikowert) wird die weitere Behandlung der Risiken festgelegt. Diese reicht von einer reinen Dokumentation bei unbedenklichem Wert (im Geschäftsjahr 2020 wahrscheinlichkeitsgewichteter Schadenwert in Höhe eines kleinen einstelligen Millionenbetrags bei der EBIT-Einbuße) über die weitere Beobachtung (Verfolgung der bestehenden Maßnahmen – bei einem Risikowert im Geschäftsjahr 2020 in Höhe eines mittleren einstelligen Millionenbetrags) bis hin zur Notwendigkeit, unverzüglich Maßnahmen zu ergreifen und zu verfolgen (Meldegrenze – bei einem wahrscheinlichkeitsgewichteten Schadenwert im Geschäftsjahr 2020 über einem mittleren einstelligen Millionenbetrag). Die so definierten Wertgrenzen werden jährlich in Abhängigkeit des geplanten Jahresergebnisses neu festgesetzt. Sofern die identifizierten Risiken quantifizierbar sind, werden die entsprechenden (stichtagsbezogenen) Risikowerte in das Berichtswesen aufgenommen.

Anschließend werden im Bedarfsfall Vorschläge für Gegenmaßnahmen erarbeitet. Der Vorstand prüft diese Maßnahmen und setzt sie zeitnah um.

Die in diesem Teil des Risikomanagements betrachteten Risiken für den secunet-Konzern und somit auch für die secunet AG als Konzernobergesellschaft werden entsprechend ihrem Ursprung in den funktionalen Bereichen der secunet hauptsächlich eingeteilt in

- Absatzrisiken: Das sind Risiken in allen Bereichen rund um die Distribution. Sie betreffen im Wesentlichen die Funktionen Einkauf und Eingangslogistik, Absatz und Ausgangslogistik sowie Vertrieb und Marketing.

- Produktrisiken: Das sind die Risiken, die im Zusammenhang mit den Produkten und Lösungen der secunet entstehen können. Sie betreffen im Wesentlichen Risiken aus technischen Defekten oder aus möglichen Sicherheitsschwächen der verwendeten Komponenten. Hinzu kommen Risiken aus den Bereichen, die für die Planung und Koordination der Marktreife von Produkten und Lösungen des secunet-Konzerns verantwortlich sind.

- Projektrisiken: Das sind die Risiken, die im Zusammenhang mit Entwicklungs- und Beratungsprojekten entstehen können. Hierzu gehören in erster Linie die Risiken der Budgetplanung sowie der darauf folgenden Budgeteinhaltung.

- Strukturrisiken: Das sind die Risiken, die sich aus Unterstützungsfunktionen wie beispielsweise Finanzen und Controlling, Recht und Personal sowie IT ergeben. Hier werden ebenfalls Risiken aus M&A-Aktivitäten sowie Compliance-Risiken erfasst.

Ein bedeutendes und durchgängig betrachtetes Risiko für die Geschäftsentwicklung im Jahr 2020 stellte darüber hinaus die Corona-Pandemie dar. Mit ihren möglichen Auswirkungen auf den secunet-Konzern befasste sich der Vorstand kontinuierlich und mit hoher Priorität. Dabei wurden alle Aspekte des Geschäftsbetriebs durchleuchtet, bewertet und wo nötig Maßnahmen entwickelt. Im Vordergrund der Erörterungen standen jeweils die Gesunderhaltung der Mitarbeitenden, die Zulieferungen durch Lieferanten und die Leistungen bei unseren Kunden sowie die eigene Infrastruktur. secunet hat sich in dieser Krisenzeit als schnell reagierende, flexible und lernende Organisation erwiesen – daher konnten Risiken im operativen Management schnell reduziert werden.

Im Laufe des Geschäftsjahres 2020 wurden im Wesentlichen Absatzrisiken identifiziert. Keines davon lag einzeln über dem oberen Grenzwert für die Unbedenklichkeit. Das jeweils umgesetzte operative Schadenmanagement konnte in allen Fällen dazu beitragen, dass der entsprechende Risikowert deutlich abgesenkt wurde.

Im Bereich der hier erörterten Absatzrisiken dominieren die Vertriebsrisiken. secunet ist im Projektgeschäft tätig: Viele Aufträge betreffen individuell gestaltete Infrastrukturen und Lösungen. Die darauf basierenden IT-Sicherheitsinfrastrukturen sind oftmals mit einem großen Investitionsvolumen verbunden. Daraus entsteht beim Kunden ein aufwendiges, oftmals langwieriges Ausschreibungs- und Entscheidungsprozedere. Dies betrifft sowohl die Kunden im Public Sector als auch diejenigen im Business Sector. Dadurch ist die Planbarkeit von Umsätzen stark eingeschränkt, entsprechend hoch ist die potenzielle Volatilität im Geschäft von secunet. Die Vertriebsrisiken werden fortlaufend im Rahmen des Risikomanagements sowie den laufenden Vorstandssitzungen überprüft, nötigenfalls wird mit adäquaten Maßnahmen gegengesteuert. Diese Maßnahmen zur Reduktion des Vertriebsrisikos bestehen oftmals darin, einen engen Kontakt und damit eine laufende Abstimmung mit dem Kunden, zum Beispiel über den Einsatz von dedizierten Key Account Managern, zu suchen. Die Vertriebsrisiken werden zum Zeitpunkt der Erstellung dieses Berichts als unbedenklich eingestuft.

Zu den Absatzrisiken gehören auch die Risiken der Lagerhaltung. Diese steigen mit dem wachsenden Produktgeschäft des secunet-Konzerns. Zu den Risiken der Lagerhaltung gehört zum einen das Risiko der kurzfristigen Lieferfähigkeit, dem durch entsprechende vernetzte Disposition (Prognose potenzieller Umsätze und Lageraufbau) begegnet wird. Zum anderen werden besonders Hardwarekomponenten aufgrund des sich beschleunigenden technischen Fortschritts obsolet. Aufgrund dieses technischen Alterungsprozesses sind gegebenenfalls Lagerbestände im Wert gemindert. secunet trägt diesen Risiken durch eine professionelle Lagerbestandsoptimierung Rechnung. Im Geschäftsjahr 2019 wurden Lagerbestände in Höhe von 0,6 Mio. Euro abgewertet.

Per Ende Dezember 2020 überwogen die Absatzchancen die Absatzrisiken um 2,6 Mio. Euro, letztere wurden daher als unbedenklich eingestuft.

Produkt-, Projekt- und Infrastrukturrisiken bestanden per Ende Dezember 2020 nicht. Insofern wurde diese Risikoklasse ebenfalls als unbedenklich eingestuft.

3.1.4 Operatives Risikomanagement

Operative Risiken werden über die spezifische Risikominimierungsroutinen erfasst, bewertet und möglichst weitgehend ausgeschlossen. Dies Kontrollmechanismen setzen an verschiedenen Stellen im Wertschöpfungsprozess an.

Vertriebs- oder Absatzrisiken werden im Rahmen der Vertriebskoordination über Risikokommissionen erörtert. Risikokommissionen sind ab einer festgelegten Auftragshöhe zwingend abzuhalten. Diese Kommissionen setzen sich mindestens aus den Vertretern des zuständigen (Vertriebs-)bereichs, der mit dem gewünschten Auftrag voraussichtlich betrauten Division / Geschäftseinheit, dem kaufmännischen Leiter, Vertretern der Rechtsabteilung und des Einkaufs sowie eines Mitglieds des Vorstands zusammen. Ziel der Risikokommissionen ist es, für den jeweiligen Auftrag oder Ausschreibung aufgrund nachvollziehbarer Kriterien zu entscheiden, ob und wie auf eine Ausschreibung geboten oder ein Auftrag angenommen werden kann. Da im Rahmen der Risikokommissionen jeweils eine Erörterung der Risiken einschließlich einer Bewertung der Tragbarkeit stattfindet und mit der Entscheidung die Risiken als akzeptabel anerkannt sind, werden die damit verbundenen Risiken zum Zeitpunkt der Erstellung dieses Berichts als beherrschbar angesehen. Neben dem bereits bei den Absatzrisiken beschriebenen Vertriebsrisiko bei Großprojekten besteht ein generelles Projektmanagementrisiko. Hinzu kommen spezielle Risiken bei sehr lange laufenden Großprojekten. Derartige Risiken werden bei secunet in der übergeordneten Projektkoordination identifiziert, bewertet und durch entsprechende Maßnahmen reduziert bzw. ausgeschaltet. Das Projektmanagementrisiko entsteht nach der Beauftragung von Großprojekten: Allein aufgrund ihrer Dimension sind diese in der Umsetzung durch vielfältige Unwägbarkeiten gekennzeichnet. Das Risiko besteht beispielsweise in der Nichteinhaltung von Terminplänen und von Projektbudgets. Diesen Risiken trägt secunet durch ein umfassendes Projektmanagement Rechnung, aus dem regelmäßig Steuerungsberichte an Projektleitung, Geschäftsbereichsleitung und Vorstand erzeugt werden. Die Risiken aus Großprojekten werden – wie auch die Entwicklungsrisiken – über umfassende Projektplanungs- und Kontrollmechanismen verbunden mit einem risikoorientierten Berichtswesen fortlaufend überwacht. Bei Abweichungen von den eingestellten Sollgrößen werden unmittelbar Maßnahmen zur Risikominderung beschlossen und umgesetzt. Diese können in der Bereitstellung von zusätzlichen Kapazitäten für die Bearbeitung des Projekts bestehen sowie in der Erörterung von Abweichungen mit den Kunden, um deren Erwartungshaltung mit den geänderten Rahmenbedingungen in Übereinstimmung zu bringen.

In sehr lange laufenden Projekten, die sich über Zeiträume von mehr als fünf Jahren erstrecken, können zudem Risiken entstehen, weil beispielsweise die dort eingesetzten Lösungen an das Ende ihrer technologischen Lebensdauer stoßen (Update-Probleme, Probleme mit veralteter Technologie). Auch können beispielsweise Lieferanten, die über die Dauer von solchen Projekten vom Markt verschwinden, ein Wiederbeschaffungsrisiko erzeugen.

Im Rahmen der Entwicklung neuer Produkte – dies sind auch entsprechende Großprojekte – werden die folgenden Risiken regelmäßig diskutiert und abgewogen:

- Das Risiko einer eventuell ausfallenden Nachfrage: Das Produkt bewährt sich nicht am Markt.
- Das Risiko technischer Fehlentwicklungen: Das Produkt weist Mängel auf, die zu Gewährleistungsansprüchen führen.
- Das Risiko der nicht rechtzeitigen Fertigstellung des Produkts: Das Entwicklungsprojekt braucht wesentlich mehr Zeit als veranschlagt.

In der Vergangenheit entwickelte secunet Produkte und Lösung im Wesentlichen als Folge von Beauftragungen zur Deckung spezifischer Sicherheitsbedarfe im öffentlichen Sektor. Die IT-Hochsicherheit orientiert sich stark an den Kundenbedürfnissen, Produkte werden grundsätzlich nicht ohne gezielte Anforderung konzipiert. Die meisten Entwicklungen von secunet sind auftragsinduziert und werden entsprechend durch die bestellenden Kunden finanziert. Entwicklungsrisiken bestehen daher nicht mit Bezug auf eine eventuell ausfallende Nachfrage. Risiken aus der Entwicklung neuer Produkte, die sich dann am Markt nicht bewähren, waren daher für secunet in den meisten Produktbereichen von untergeordneter Bedeutung.

Die Entwicklung des secunet konnektors für Arztpraxen im Geschäftsjahr 2018, die Entwicklung des secunet Communicator im Public Sector sowie des Rechenzentrumskonnektors und secunet edge im Business Sector im Jahr 2019 und die Entwicklung des secunet Communicator, des easykiosk und der Lösung protect4use im Jahr 2020 haben das Volumen der damit verbundenen eigenen Investitionen steigen lassen. Damit sind Entwicklungsrisiken stärker in den Fokus der Risikoevaluierung geraten. Hierbei sind weniger die mit den Produkten verbundenen Absatzaussichten als die Dauer von Entwicklung und Zulassung im Fokus. Das größte Risiko bei Entwicklungsprojekten kann in der Unterschätzung des notwendigen Zeitbedarfs bis zur Abnahmereife bestehen. Dadurch können Zeit- und Personalaufwendungen entstehen, welche die Profitabilität des Projekts beschränken. Um diese Risiken möglichst gering zu halten, setzt secunet an verschiedenen Stellen umfassende Projektplanungs- und Kontrollmechanismen, verbunden mit einer dezidierten Berichtslinie, ein. Dieser Teil der Risikoanalyse und des Risikomanagements deckt sich mit den Aktivitäten, die sich auf Großprojekte beziehen.

Für den Bereich der Entwicklungsprojekte wird das Risiko zum Zeitpunkt der Erstellung dieses Berichts als gering eingestuft.

Projektrisiken bestanden per Ende Dezember 2020 nicht, entsprechend wurde diese Risikoklasse als unbedenklich eingestuft.

Das Produktportfolio der secunet AG fokussiert auf Lösungen im Bereich der Cyber Security, speziell sind dies im Falle der SINA-Produktfamilie kryptografisch auf hohem Niveau abgesicherte und zugelassene Lösungen.

Ein Risiko, das im Zusammenhang mit den technischen Eigenschaften dieser Produkte laufend begutachtet wird, ist die Auswirkung von möglichen – bisher unentdeckten – Sicherheitsschwächen dieser Lösungen. Hier wird der Frage nachgegangen, ob und inwieweit durch Sicherheitslücken in einzelnen Komponenten das mit der Gesamtlösung verbundene Sicherheitsversprechen der secunet an ihre Kunden eventuell kompromittiert wird. Dies ist die Aufgabe im operativen Incident Management, einer weiteren Komponente des Risikomanagements bei secunet.

Zur Risikominimierung findet in diesem Bereich ein umfassender Prozess der fortlaufenden Risikoidentifizierung und -evaluierung statt. Dabei werden Erkenntnisse aus verschiedensten Quellen über potenzielle Sicherheitsrisiken durch secunet gesammelt und bewertet. Sofern im Ergebnis dieser Bewertung auch nur eine eventuelle Angreifbarkeit der Systeme möglich erscheint, werden die Kunden unverzüglich in Kenntnis gesetzt und bei der Schließung der potenziellen Sicherheitslücke unterstützt.

Dieser Prozess der Überwachung und Lösung potenzieller technischer Sicherheitsrisiken wird in enger Abstimmung mit dem Entwicklungs- und Zulassungspartner Bundesamt für Sicherheit in der Informationstechnik (BSI) umgesetzt.

Vor dem Hintergrund der praktizierten Risikominimierungsmaßnahmen wird das wirtschaftliche Risiko der technischen Produktsicherheit als gering eingeschätzt.

3.2 Chancen

Unverändert wirken sich die nachfolgend beschriebenen Treiber positiv auf das zukünftige Wachstum von secunet aus:

3.2.1 Wachstum über zunehmende Sensibilisierung

Die zunehmende Sensibilisierung der letzten Jahre für Fragen der IT-Sicherheit wurde unter anderem durch verschiedene Berichte zu Cyber-Security-Bedrohungen (wie beispielsweise Abhöraffären, versuchtes und erfolgreiches Hacking von Behörden- und Unternehmensnetzen, Angriffe auf kritische Infrastrukturen) medial stark unterstützt.

Untersuchungen zur mittel- bis langfristigen Einschätzung von Risiken bei Unternehmen und Entscheidern ergeben zudem, dass Cyber Security eine deutlich steigende Bedeutung zugemessen wird. Das Thema Cybersicherheit steht weithin im Fokus verschiedenster Untersuchungen und Tagungen sowie daraus abgeleiteten Veröffentlichungen. Cybervorfälle stehen zunehmend im Fokus der Risikobetrachtungen, nicht nur von Behörden, sondern auch von Unternehmen der privaten Wirtschaft. So werden zum Beispiel im Allianz Risk Barometer der Top Business Risks in Deutschland der vergangenen drei Jahre Cybervorfälle durchgängig unter den bedeutendsten drei Risiken genannt. Das gleiche Bild ergibt sich in der globalen Betrachtung. Auch der Global Risk Report 2021 des World Economic Forum listet Cyberattacken und die Verwundbarkeit von IT-Infrastrukturen unter den Top 10 Risiken weltweit.

Hieraus kann ein positiver Trend für die Nachfrage nach hochwertigen und vertrauenswürdigen IT-Sicherheitslösungen „made in Germany“ abgeleitet werden. Dies betrifft sowohl Behörden, die ihre bestehenden Anstrengungen um Sicherheit der IT-Systeme und -Infrastrukturen noch ausweiten, als auch Unternehmen, die dem konkret gewordenen Risiko, zum Beispiel der Wirtschaftsspionage, entsprechende Schutzmaßnahmen entgegensetzen. Hinzu kommen verstärkt Betreiber kritischer Infrastrukturen, für die IT-Sicherheit immer wichtiger wird (siehe auch „Wachstum aufgrund zunehmender Regulierung“). Durch entsprechende vertriebliche Aktivitäten im Behörden- und Unternehmensbereich zielt secunet darauf, an dieser positiven Nachfrageentwicklung zu partizipieren.

Das zunehmende Interesse an IT-Sicherheit, unter anderem getrieben durch die hohe mediale Aufmerksamkeit, und die in der Folge wachsende Nachfrage ziehen auch einen zunehmenden Wettbewerb nach sich. Dieser ist bei der Bewertung der Chancen mit zu berücksichtigen.

3.2.2 Wachstum über zunehmende Regulierung

Die deutsche Bundesregierung will den Schutz kritischer Infrastrukturen wie Energie- und Telekommunikationsnetze sowie von IT-Systemen erhöhen. Sie hat dazu im Juli 2015 das IT-Sicherheitsgesetz erlassen. Wachstumstreiber ergeben sich daraus auf verschiedenen Ebenen:

- Das Gesetz betrifft besonders die Betreiber kritischer Infrastrukturen, also von Einrichtungen, die für das Gemeinwesen von zentraler Bedeutung sind, wie zum Beispiel die Energieversorgung. Sie sollen spezifische Anforderungen an die IT-Sicherheit erfüllen. Hieraus entsteht potenzielle Nachfrage nach Umsetzungskonzepten für diese Anforderungen.

- Des Weiteren ist die Rolle des BSI durch das Gesetz gestärkt worden und trägt seiner gewachsenen Bedeutung als zentrale Stelle für die IT-Sicherheit Rechnung. Unter anderem hat das BSI die Befugnis erhalten, auf dem Markt befindliche IT-Produkte und -Systeme im Hinblick auf ihre IT-Sicherheit zu prüfen, zu bewerten und die Ergebnisse bei Bedarf zu veröffentlichen. Hieraus können sich positive Impulse auf das Produktgeschäft der secunet ergeben.

Im Dezember 2020 hat die deutsche Bundesregierung den Entwurf für das IT-Sicherheitsgesetz 2.0 beschlossen. Die Weiterentwicklung des Gesetzes sieht eine Stärkung des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Verbraucherschutzes, der unternehmerischen Vorsorgepflichten und der staatlichen Schutzfunktion vor.

3.2.3 Wachstum über neue Märkte

IT-Sicherheitslösungen „made in Germany" erfreuen sich weltweit aufgrund ihrer Qualität und Vertrauenswürdigkeit eines guten Rufs. Die internationale Nachfrage nach entsprechenden hochwertigen Lösungen, wie sie auch secunet anbietet, wächst.

Unter dem Eindruck von Abhöraffären und Cyberattacken dürfte die Nachfrage noch deutlichere Unterschiede nach Herstellerländern machen, von denen secunet als deutscher Hersteller profitiert. Hinzu kommen die Zulassungen von secunet-Produkten für den Einsatz im internationalen Kontext, beispielsweise bei der EU und der NATO.

Das Angebot für Kunden im industriellen Sektor durch den Geschäftsbereich Business Sector soll auch im Ausland ausgeweitet werden, beispielsweise für ausländische Tochtergesellschaften und Produktionsstätten deutscher Konzerne. Hierzu werden vielversprechende Potenziale identifiziert und geprüft.

Der Ausbau der Auslandsaktivitäten über den secunet-eigenen Vertrieb sowie über lokale Multiplikatoren soll dazu beitragen, diese Potenziale zu heben.

3.2.4 Wachstum durch Zukäufe

Neben dem organischen Wachstum auf Inlands- wie Auslandsmärkten verfolgt secunet seit Jahren das Ziel, über M&A-Aktivitäten weiteres Wachstum herbeizuführen. Vielversprechend ist der Zuwachs im Produktbereich über den Erwerb von entsprechenden Lösungsanbietern. Der Markt für Unternehmen mit hochwertigen, zugelassenen IT-Sicherheitslösungen für die Bearbeitung von Verschlusssachen, auf dem secunet tätig ist, ist in viele kleine bis mittlere Anbieter zersplittert. Zudem ist das M&A-Geschäft auch weiterhin durch sehr hohe Preisvorstellungen seitens der Verkäufer geprägt. Der Prozess der Identifizierung erfolgversprechender und preislich akzeptabler Targets ist entsprechend aufwendig, wird aber dennoch kontinuierlich verfolgt.

3.3 Gesamtbild aus Risiken und Chancen

Eine zusammenfassende Betrachtung der Chancen und Risiken, welche die weitere Entwicklung des secunet-Konzerns beeinflussen könnten, führt zu einer insgesamt zuversichtlichen Einschätzung.

Die Beurteilung hat ergeben, dass die Risiken zum Zeitpunkt der Erstellung dieses Berichts insgesamt unbedenklich und damit beherrschbar sind, und die identifizierten Risiken einzeln und in ihrer Gesamtheit keine den Fortbestand des Konzerns und des Unternehmens gefährdenden Risiken im Hinblick auf Illiquidität oder Überschuldung im Berichtszeitraum von mindestens einem Jahr darstellen. Im operativen Management des Konzerns werden durchgängig Maßnahmen ergriffen, die eine Steigerung der Risikoposition verhindern sollen. Zugleich wird mit einer Vielzahl von Aktivitäten die Nutzung der beschriebenen Chancen vorangetrieben. Zum Bilanzstichtag liegen keine wesentlichen Risiken vor.

Die Geschäftsentwicklung der secunet AG unterliegt den gleichen Risiken und Chancen wie die des Konzerns. Daher gilt die Darstellung und Würdigung der Risiken und Chancen analog für die secunet AG.

3.4 Prognosebericht

Im abgelaufenen Geschäftsjahr sind Umsatzerlöse und EBIT zum wiederholten Male kräftig angestiegen, in der Folge ist das Jahr 2020 mit hervorragendem Ergebnis abgeschlossen worden. Der Vorstand der secunet AG sieht die Voraussetzungen für eine gute Geschäftsentwicklung für das laufende Jahr 2021 grundsätzlich optimistisch.

Die Rahmenbedingungen für das Geschäftsjahr 2021 stimmen optimistisch:

- Die gesamtwirtschaftlichen Wachstumsaussichten der deutschen Bundesregierung sind positiv: Für das laufende Jahr 2021 wird ein Wachstum des preisbereinigten Bruttoinlandsprodukts um 3,0 % erwartet.

- Für den Inlandsmarkt rechneten wir auch weiterhin mit einer wachsenden Nachfrage nach IT-Sicherheit. Dies betrifft sowohl den Public Sector, also das Geschäft mit öffentlichen Auftraggebern, als auch den Business Sector, der Unternehmen der privaten Wirtschaft sowie den Gesundheitssektor bedient. Für das Jahr 2021 prognostiziert Bitkom ein Wachstum der Ausgaben für Hardware, Software und Services in der Informationstechnik um 4,2 % auf 4,9 Mrd. Euro. Der Markt für IT-Sicherheit dürfte relativ stärker wachsen. secunet wird diese wachsende Nachfrage auch in Zukunft mit optimierten und neuen Dienstleistungen, Produkten und Lösungen gut befriedigen können.

- Der Auslandsmarkt birgt unverändert signifikante Wachstumspotenziale: Um diese zu heben, ist secunet prinzipiell gut aufgestellt. Die im internationalen Vertrieb tätigen Mitarbeiter der secunet AG und der secunet International GmbH & Co. KG können sich auf eine mehrjährige Erfahrung im Konzern und im Umgang mit internationalen Kunden stützen.

- Im Laufe des letzten Jahres hat der secunet-Konzern die Zahl seiner produktiven Mitarbeiter erneut gesteigert und kann somit steigende Nachfrage und hohe Kapazitätsauslastung in gute Geschäftsergebnisse umsetzen.

- Die unveränderten Bestrebungen, nationale wie internationale Verteidigungshaushalte mit dem Fokus auf Cyber Defence auszuweiten, begründen positive Wachstumserwartungen.

Der Vorstand erachtet den secunet-Konzern und die secunet AG zum Zeitpunkt der Erstellung dieses Berichts als gut aufgestellt und die Lage der Gesellschaft und des Konzerns ist aus der Sicht der Unternehmensleitung nach wie vor gut:

- Der secunet-Konzern und die secunet AG stehen wirtschaftlich und finanziell gut da: Das bisherige Wachstum wurde profitabel erreicht, es bestehen keine Kredite, und der Bestand an liquiden Mitteln ist hoch.

- Der Vorstand ist der Ansicht, dass secunet über leistungsfähige, motivierte und ausgezeichnet qualifizierte Mitarbeiter verfügt und damit eine hervorragende Grundlage an Knowhow gegeben ist.

- Das bestehende Produkt- und Leistungsportfolio der Gesellschaft hat sich im Wettbewerb gut bewährt und wird fortlaufend in enger Abstimmung mit den Kunden und ihren Bedürfnissen ausgeweitet. Hinzu kommen Erweiterungen der Produktpalette, die auch zukünftiges Wachstum stützen.

- secunet vertritt die Ansicht, dass die Produkte und Lösungen von secunet einen ausgezeichneten Ruf haben, das Unternehmen als Lieferant von hochwertiger und vertrauenswürdiger IT-Sicherheit für höchste Ansprüche anerkannt ist und daher eine stabile und zuverlässige (Bestands-)Kundenstruktur hat.

Gleichwohl bestehen mit Blick auf das kommende Jahr auch Risiken:

- secunet ist weiterhin stark abhängig von der Beschaffungsaktivität der deutschen Bundesbehörden. Auswirkungen, die aus einer sich verändernden Haushaltspolitik herrühren, können derzeit noch nicht eingeschätzt werden. Eine negative Folge für secunet könnte die Verschiebung oder Streichung von geplanten Projekten sein.

- Das Projektgeschäft birgt ebenso viele Chancen wie Risiken: Der Umfang der Investitionsentscheidung bei Großprojekten, zumal wenn diese in einen politischen Prozess eingebunden sind, kann den Eintritt erwarteter Beschaffungen deutlich verzögern. Außerdem bergen laufende Großprojekte auch immer das Risiko vorab nicht kalkulierbarer Verzögerungen oder Budgetüberschreitungen.

- Die hohe Aufmerksamkeit, die sich auf IT-Sicherheit als Thema richtet, schürt einerseits die Erwartung steigender Nachfrage. Davon angezogen wird andererseits auch ein zunehmender Wettbewerb, dessen Auswirkungen nicht absehbar sind.

Die im Geschäftsjahr 2020 erreichten sehr hohen Geschäftsergebnisse stellen eine Herausforderung für weiteres Wachstum dar – die Überschreitung der fortgesetzten Rekordergebnisse wird zunehmend anspruchsvoller. Sonderkonjunkturen wie im Geschäftsjahr 2019 im Gesundheitswesen (ausgelöst durch den Rollout der Gesundheitskonnektoren in den Arztpraxen) oder im Geschäftsjahr 2020 im öffentlichen Sektor (hohe Investitionen in mobile Arbeitsplätze) sind für das Geschäftsjahr 2021 nicht zu erwarten.

Daher hat der Vorstand der Gesellschaft seine Prognose für den secunet-Konzern für das kommende Geschäftsjahr 2021 bereits am 3. November 2020 wie folgt veröffentlicht: gerechnet wird mit Umsatzerlösen um 260 Mio. Euro und einem Ergebnis vor Zinsen und Steuern (EBIT) um 38 Mio. Euro. Der Beitrag der Geschäftsbereiche Public Sector und Business Sector zu den Konzern-Umsatzerlösen im Jahr 2021 wird voraussichtlich nicht

wesentlich von demjenigen im Jahr 2020 abweichen. Für den Business Sector erwarten wir ein leicht positives EBIT.

Für die Prognose der secunet AG gelten die gleichen Annahmen wie für den secunet-Konzern. Entsprechend erwartet der Vorstand für die secunet AG einen leichten Rückgang von Umsatz und EBIT.

4. Risikoberichterstattung in Bezug auf die Verwendung von Finanzinstrumenten

Das Finanzmanagement der Gesellschaft und des Konzerns orientiert sich grundsätzlich an den gesellschaftsrechtlichen Bestimmungen und Erfordernissen. Damit wird sichergestellt, dass alle Konzernunternehmen unter der Unternehmens- fortführungsprämisse operieren können. Der Konzern und seine Gesellschaften waren jederzeit in der Lage, ihren Zahlungsverpflichtungen nachzukommen. Die Anlage der liquiden Mittel erfolgt streng risikominimierend. Das laufende Monitoring der liquiden Mittel und die Abstimmung mit dem Liquiditätsbedarf dienen der dauerhaften Sicherstellung der Zahlungsfähigkeit. Dies ist auch das oberste Ziel des Finanzmanagements.

5. Beschreibung der wesentlichen Merkmale des rechnungslegungsbezogenen internen Kontroll- und Risikomanagementsystems (§289 Absatz 4 und §315 Absatz 4 HGB)

5.1 Elemente des internen Kontroll- und Risikomanagementsystems

Das interne Kontrollsystem im secunet-Konzern umfasst alle Grundsätze, Verfahren und Maßnahmen zur Sicherung der Wirksamkeit, Wirtschaftlichkeit und der Ordnungsmäßigkeit der Rechnungslegung und sichert ebenfalls die Einhaltung der maßgeblichen rechtlichen Vorschriften.

Im secunet-Konzern besteht das interne Kontrollsystem aus dem internen Steuerungs- und dem internen Überwachungssystem. Der Vorstand der secunet AG – mit seiner Organfunktion zur Führung der Geschäfte – hat die in der secunet Service GmbH geführten Bereiche Controlling, Finanzen sowie Recht und Personal als Verantwortliche des internen Steuerungssystems im secunet-Konzern beauftragt.

Prozessintegrierte und prozessunabhängige Überwachungsmaßnahmen bilden die Elemente des internen Überwachungssystems im secunet-Konzern.
Neben manuellen Prozesskontrollen – wie dem Vier-Augen-Prinzip – sind auch die maschinellen IT-Prozesskontrollen ein wesentlicher Teil der prozessintegrierten Maßnahmen. Weiterhin werden durch Gremien wie den Risikoausschuss sowie durch spezifische Konzernfunktionen wie den Bereich Recht prozessintegrierte Überwachungen sichergestellt.

Das hier dargestellte Risikomanagementsystem richtet sich im Wesentlichen auf die Vermeidung des Eintretens von Schäden durch Risiken.

Die interne Revision der secunet AG ist mit prozessunabhängigen Prüfungstätigkeiten in das interne Überwachungssystem im secunet-Konzern eingebunden.

5.2 Einsatz von IT-Systemen

Die Erfassung buchhalterischer Vorgänge erfolgt bei der secunet AG im Wesentlichen durch das ERP-System des Herstellers SAP.

5.3 Spezifische konzernrechnungslegungsbezogene Risiken

Spezifische konzernrechnungslegungsbezogene Risiken können sich z.B. aus dem Abschluss ungewöhnlicher oder komplexer Geschäfte ergeben sowie aus Geschäftsvorfällen, die nicht routinemäßig bearbeitet werden.

5.4 Wesentliche Regelungs- und Kontrollaktivitäten zur Sicherstellung der Ordnungsmäßigkeit und Verlässlichkeit der Rechnungslegung im Konzern

Die Kontrollaktivitäten zur Sicherstellung der Ordnungsmäßigkeit und Verlässlichkeit der Rechnungslegung umfassen z.B. die Analyse von Sachverhalten und Entwicklungen anhand spezifischer Kennzahlenanalysen. Die Trennung von Verwaltungs-, Ausführungs-, Abrechnungs- und Genehmigungsfunktionen und deren Wahrnehmung durch verschiedene Personen reduzieren die Möglichkeit zu dolosen Handlungen. Die organisatorischen Maßnahmen sind auch darauf ausgerichtet, Umstrukturierungen oder Veränderungen in der Geschäftstätigkeit einzelner Geschäftsbereiche zeitnah und sachgerecht in der Konzernrechnungslegung zu erfassen. Weiterhin ist z.B. sichergestellt, dass bei Veränderungen in den eingesetzten IT-Systemen der zugrundeliegenden Buchführungen in den Konzerngesellschaften eine periodengerechte und vollständige Erfassung buchhalterischer Vorgänge erfolgt. Das interne Kontrollsystem gewährleistet auch die Abbildung von Veränderungen im wirtschaftlichen oder rechtlichen Umfeld des secunet-Konzerns und stellt