Von links: Stefan Kinnen, DOAG-Vorstand, Norbert Drecker und Michael Sieben, beide sind Geschäftsführer der TWINSEC GmbH

Sicherheitsvorfälle zeigen, dass sich viele Unternehmen der großen Bedeutung von IT-Security immer noch nicht bewusst sind. Stefan Kinnen, DOAG-Vorstand, und Wolfgang Taschner, Chefredakteur der DOAG *News*, sprachen darüber mit Michael Sieben und Norbert Drecker, beide sind Geschäftsführer der TWINSEC GmbH.

„Die Kunst besteht darin, Risiken und Maßnahmen richtig einzuschätzen …“

Wie ist das Geschäftsmodell Ihres Unternehmens?

Sieben: Wir beraten Unternehmen herstellerneutral und produktunabhängig und setzen anschließend die gemeinsam erarbeiteten Konzepte für einen sicheren Betrieb in der IT um. Unsere Dienstleistung beginnt mit einer Analyse, danach zeigen wir anhand der Anforderungen des Kunden entsprechende Lösungswege auf, die wir bei Bedarf auch implementieren und managen.

Was bedeutet IT-Security für Sie?

Drecker: IT-Security ist eine Geschäftsgrundlage genauso wie beispielsweise eine ausreichende Kapitalausstattung. Das heißt, dass die IT-Security-spezifischen Prozesse im Unternehmen implementiert, ausgeführt und kontrolliert werden müssen.

Sieben: Entscheidend ist, dass man die IT-Security ganzheitlich und mit der gleichen Priorität wie die anderen Geschäftsprozesse behandelt.

Auf welche bedeutenden Referenzen können Sie mit Ihrem Unternehmen verweisen?

Sieben: Wir sind sehr erfolgreich in den Bereichen vertreten, in denen eine hohe Anforderung an die Sicherheit besteht. Dazu zählen Banken und Versicherungen sowie die Telekommunikationsbranche, aber auch der gehobene Mittelstandsbereich.

Drecker: Gerade im Mittelstand kann ein Sicherheitsleck die Existenz eines ganzen Unternehmens bedrohen.

Sehen Sie bezüglich IT-Security große Unterschiede in den einzelnen Branchen?

Sieben: Die Anforderungen sind zunächst in jeder Branche annähernd gleich. Bei der Gewichtung hingegen gibt es große Unterschiede, sei es durch die Gesetzgebung oder durch Revisionsvorgaben. Außerdem ist der Level an IT-Security jedes Mal anders; ein kleines Unternehmen kann nicht die gleichen Mittel einsetzen wie ein großes.

Was ist die größte Motivation der Kunden, sich mit IT-Security zu beschäftigen?

Drecker: Vor fünf bis zehn Jahren hat man sich dem Thema von der technischen Seite her genähert und Dinge wie User-Provisioning oder Single Sign-on eingeführt. Heute ist IT-Security schlicht und einfach eine Geschäftsanforderung. Banken und Versicherungen beispielsweise müssen gegenüber ihren gesetzlich vorgeschriebenen Instanzen Rechenschaft ablegen.

Sieben: Der Mittelstand hat IT-Security immer sehr stiefmütterlich behandelt. Im Rahmen der Globalisierung muss er sich heute intensiv damit auseinandersetzen.

Wie gehen Sie bei Kunden-Projekten vor?

Drecker: Das Erste und Wichtigste ist das Stellen der richtigen Fragen und das Zuhören, wenn der Kunde über seine Geschäftsprozesse berichtet. Daraus erstellen wir gemeinsam die entsprechenden Anforderungen, aus denen sich dann die praktische Umsetzung ableitet. Unsere oberste Priorität ist es, Lösungen zu erstellen, und nicht bestimmte Produkte zu verkaufen.

Sieben: Häufig ist es erforderlich, vorab gemeinsam die ganzen IT-Security-Begriffe abzuklären, damit wir alle eine gemeinsame Sprache sprechen. Das ist insofern wichtig, als IT-Fachleute meist unter einem bestimmten Schlagwort etwas anderes verstehen als die Controller oder die Mitarbeiter aus den Fachabteilungen.

Welche Abteilungen sollten bei einem IT-Security-Projekt einbezogen werden?

Sieben: Zunächst einmal gibt es immer einen Treiber für die IT-Security. Das kann der Betrieb sein, oftmals sind es auch die Controller oder die Geschäftsleitung. Danach werden die Kreise sehr schnell größer, denn vom Thema IT-Security ist jeder Bereich im Unternehmen betroffen. Die große Kunst besteht darin, alle Beteiligten einzubinden.

Sind sich die Abteilungen auch einig, wer die Kosten für die IT-Security-Maßnahmen trägt?

Drecker: Nein, die Finanzierung ist meist ein aufwändiger Prozess. Der Bereich, der die Anforderungen stellt, ist häufig nicht bereit oder in der Lage, die Kosten zu übernehmen. Der IT-Security-Beauftragte eines Unternehmens verfügt meistens gar nicht über das entsprechende Budget.

Wie stellt man in der Praxis sicher, dass die User nur die Daten sehen, die sie auch sehen sollen?

Drecker: Es gibt einmal die klassischen Instrumente wie beispielsweise eine Firewall. Unter modernen Aspekten betrachtet greifen hier auch entsprechende Berechtigungskonzepte. Das Information Rights Management geht ebenfalls in diese Richtung, setzt allerdings voraus, dass im Unternehmen klassifizierte Daten vorliegen.

Sieben: Die Palette an Möglichkeiten ist so breit wie das Thema. Das geht bis in Bereiche wie Kryptologie oder Datenbank-Automatismen, die einzelne Felder einer Tabelle kontrollieren. Entscheidend für den Einsatz sind auch hier wieder die Anforderungen des Unternehmens.

Ist der Aufbau von Sicherheit nur ein rein technisches Problem oder muss man dabei auch die Organisation des Unternehmens betrachten?

Sieben: Die Organisation wird häufig vernachlässigt, beispielsweise wenn ein Mitarbeiter die Abteilung wechselt und seine alten Rechte beim Datenzugriff mitnimmt. Hier helfen technische Maßnahmen nicht weiter, hier sind organisatorische Prozesse gefragt. Das kann bis hin zu Änderungen in der Organisationsstruktur führen.

Wann beziehungsweise wie ist ein Monitoring von auffälligen Zugriffen sinnvoll?

Drecker: Ein Ansatz besteht darin, alle Risiken für das Geschäft zu betrachten und zu analysieren. Dann kommt das IT-Security Information and Event Management (SIEM) ins Spiel. Ziel ist es, für alle sicherheitsrelevanten Vorfälle entsprechende Maßnahmen zu erstellen, die auch mit dem Geschäft in Einklang stehen. Für eine Bank wäre es beispielsweise fatal, bei einer IT-Security-Attacke das System komplett herunterzufahren. Die Kunst besteht darin, Risiken und Maßnahmen richtig einzuschätzen und in ihren Folgen entsprechend zu bewerten.

Michael Sieben, Geschäftsführer der TWINSEC GmbH

Sieben: Betriebssysteme, Datenbanken und Anwendungen sind gar nicht dafür ausgelegt, nicht erlaubte Zugriffe erkennbar zu machen. Auch SIEM-Systeme sind heute noch sehr technisch orientiert. Wenn beispielsweise ein Anwender für eine bestimmte Applikation autorisiert ist und von einem bestimmten Ort aus darauf zugreift, ist das technisch für das System in Ordnung. Wenn der gleiche Anwender aber zur selben Zeit auch noch von einem anderen Ort aus zugreift, stimmt etwas nicht. In solchen Fällen hilft nur die intelligente Korrelation der Daten weiter. Diese Denkweise ist bei vielen Unternehmen noch nicht angekommen. Gefahrenabwehr lässt sich nicht allein technisch lösen.

Zur Person: Norbert Drecker

Norbert Drecker ist seit dem 1. Januar 2008 geschäftsführender Gesellschafter der TWINSEC GmbH. Das Unternehmen, dessen Mitgründer er ist, fokussiert sich auf das Thema „IT-Sicherheit" und berät, implementiert und betreut Lösungen auf Basis verschiedener Hersteller.

Seinen beruflichen Werdegang startete er nach dem Abschluss des Studiums der Informatik an der Universität Paderborn beim EDV-Hersteller Bull. Dort sammelte er zunächst Erfahrungen in der Entwicklung von System- und Anwendungs-Software mit Schwerpunkt „Telekommunikation auf Mainframes und Minicomputern". Sein Aufgabenbereich verlagerte sich später auf konzeptionelle Aufgaben, Methoden und Projektmanagement.

Als Mitarbeiter der Evidian verantwortete er dann den technischen Bereich als Leiter des Evidian Competence Centers. In seiner Verantwortung wurden Projekte zum Thema „System & Netzwerk-Management bei Behörden" in der Telekommunikationsbranche und der Industrie konzipiert und umgesetzt. In den letzten Jahren erfolgte dann die Spezialisierung auf die IT-Sicherheit mit den breiten Themenbereichen „Compliance" und „Identity/Access-Management" mit Referenzprojekten in Umgebungen von Transport, Logistik, Telekommunikation, Verwaltung, Versicherung und Industrie in mittleren und großen Organisationen.

Das Interesse an der Vielfalt des Themas „IT-Sicherheit" und der Erfolg bei der Arbeit mit Analysten, Partnern und Produktlieferanten führte zu dem Entschluss, mit einem Team erfahrener Spezialisten diese Arbeit in einem eigenen unabhängigen Unternehmen weiter zu führen. Norbert Drecker verantwortet nun in der TWINSEC GmbH den technischen Bereich der Beratung, der Umsetzung und den Betrieb von IT-Security-Lösungen.

Wie kann man Test- und Integrationsumgebungen sicher aufsetzen?

Drecker: Dafür gibt es in der Datenbank-Technologie zunächst einige Standard-Methoden, beispielweise die Testdaten von den Echtdaten zu separieren oder die Testdaten zu maskieren und zu anonymisieren. Darüber hinaus ist die Passwort-Thematik in einem Testsystem gesondert abzubilden.

Wie sollte man mit Vorfällen im Unternehmen umgehen?

Sieben: In dem Moment, in dem etwas vorfällt, muss anhand des Maßnahmenkatalogs bereits eine entsprechende Reaktion feststehen. Es ist zudem wichtig, die Existenz dieses Maßnahmenkatalogs im Unternehmen zu propagieren, damit die Mitarbeiter wissen, dass Vorfälle entsprechend geahndet werden. Schließlich kommen rund drei Viertel aller Attacken aus dem Unternehmen und nicht von außen.

Drecker: Mit dem Maßnahmenkatalog ist es wie bei einer Feuerwehr-Übung. Jeder Beteiligte muss im Ernstfall wissen, was und wie er etwas zu tun hat.

Wie ist die Einbindung des Betriebsrats und des Datenschutzbeauftragten in die Prozesse?

Drecker: Die Einbindung ist unumgänglich. Betriebsrat und Datenschutzbeauftragte sind in die Prozesse einzubeziehen.

Wo sind sinnvolle Grenzen von IT-Security-Maßnahmen?

Drecker: Wie gesagt, zu Beginn aller IT-Security-Aktivitäten steht die Risiko-Analyse. Danach ist man in der Lage zu beurteilen, an welcher Stelle Maßnahmen zu ergreifen sind. Erst wenn alle Risiken erkannt sind, lässt sich eine Kosten/Nutzen-Rechnung aufmachen. Der Vorstand muss dann entscheiden, welche Risiken er in Kauf nimmt, um Kosten für bestimmte Maßnahmen zu sparen.

Welche Trends kommen kurz- und mittelfristig auf uns zu?

Drecker: Vor fünf bis sieben Jahren stand noch die technische Umsetzung von Sicherheitsmaßnahmen im Fokus. Die Diskussion fand meist unter dem Aspekt des Return on Investment statt. Heute geht es vorrangig um Compliance. Gesetzliche Anforderungen sowie die aus der Firmenpolitik entstehenden Ansprüche sind in einem Sicherheitskonzept umzusetzen. Dabei ist der Nachweispfad von drei Säulen abhängig. Einer macht die Vorgaben, einer setzt sie um und ein Dritter kontrolliert das Ganze. Dieser Trend, der momentan in erster Linie bei den DAX-Unternehmen praktiziert wird, hat künftig auch im Mittelstand eine große Bedeutung. Hier wird sich noch ein großer Markt entwickeln.

Norbert Drecker, Geschäftsführer der TWINSEC GmbH

Sieben: IT-Security muss zu einer Selbstverständlichkeit im Unternehmen werden, unabhängig von dessen Größe. Gerade hinsichtlich neuer Technologien wie Cloud Computing oder Mobile Applications sind aufgrund der wachsenden Komplexität noch große Aktivitäten erforderlich. Gerade bei den mobilen Anwendungen ist der Markt extrem schnelllebig geworden. Die Anforderungen hinsichtlich Mobilität werden meist umgesetzt, ohne sich große Gedanken um die damit verbundene Sicherheit zu machen.

Wie schätzen Sie die Aktivitäten Oracles hinsichtlich IT-Security ein?

Sieben: Die Vollständigkeit der Lösungen ist beeindruckend, lediglich bei SIEM besteht noch Nachholbedarf. Hinsichtlich der Marktdurchdringung hat Oracle durch eine gezielte Informationspolitik sicher noch Steigerungspotenzial, insbesondere im deutschen Markt.

Welche Rolle sollte die DOAG bei der IT-Security spielen?

Sieben: Die DOAG bietet die Plattform, auf der die Anwender ihre Probleme kommunizieren können. Sie ist dann in der Lage, diese zu bündeln und dem Hersteller Lösungsvorschläge zu unterbreiten.

Welche konkreten Wünsche haben Sie an den Markt?

Drecker: Erst mal sollte die IT-Security den Stellenwert im Unternehmen bekommen, den auch die anderen Bereiche innehaben. Zum anderen fehlt mir bei den Mitarbeitern oft noch das entsprechende Bewusstsein für Sicherheit.

Gibt es eine absolute Sicherheit?

Sieben: Nein. IT-Security bleibt immer ein Wettrennen zwischen den Möglichkeiten, die ein Angreifer nutzt, und den Mechanismen, die es zum Schutz gibt. Das Optimum wird immer ein Kompromiss bleiben.

Zur Person: Michael Sieben

Michael Sieben ist seit dem 1. Januar 2008 geschäftsführender Gesellschafter der TWINSEC GmbH. Neben dieser Tätigkeit ist er verantwortlich für die Bereiche Vertrieb sowie Kunden- und Projekt-Management. Bis zu seiner Beteiligung an der neu gegründeten TWINSEC GmbH war er Leiter Vertrieb Zentraleuropa und stellvertretender Geschäftsführer bei der Evidian GmbH. Nach seiner kaufmännischen Ausbildung mit anschließendem Traineeprogramm der IBM arbeitete Michael Sieben als Account Manager, Key Account Manager und Teamleiter bei der IBM Deutschland GmbH und der ELEKLUFT GmbH (Tochter der DASA) in Bonn. In dieser Zeit unterstützte und betreute er geheimhaltungsbedürftige öffentliche Kunden sowie Versicherungsunternehmen in zahlreichen Großprojekten und war zum Zugang schützenswerter Einrichtungen und Projekte ermächtigt und betraut.
Als Mitarbeiter der Evidian verantwortete er dann den Vertrieb für Zentraleuropa. In seiner Betreuung und Beratung wurden Projekte zum Thema „System & Netzwerk-Management bei Behörden" in der Telekommunikationsbranche und der Industrie umgesetzt. In den letzten Jahren erfolgte dann die Spezialisierung auf die IT-Sicherheit mit den breiten Themenbereichen „Compliance" und „Identity/Access-Management" mit Referenzprojekten in Umgebungen von Transport, Logistik, Telekommunikation, Verwaltung, Versicherung und Industrie in mittleren und großen Organisationen. Seine Fachgebiete sind System- und Netzwerk-Management, ITIL, IT-Security, Identity und Access-Management, Compliance, Rollen-Management, BSI-Grundschutz, Workflow-Systeme und Managed Security Services. Michael Sieben ist Vollkaufmann mit einigen Zusatz-Semestern der technischen Informatik an der Fernuniversität Hagen.