Managementwissen kompakt

Datensicherheit als elementarer Baustein der Wertschöpfungskette für die Chemie- und Pharmabranche

Ein Service-Whitepaper von

apsec applied security

Applied Security GmbH • Einsteinstraße 2a • 63868 Großwallstadt
www.apsec.de • info@apsec.de • Fon: +49 (0) 60 22 / 263 38-0

apsec applied security

Applied Security GmbH
Einsteinstraße 2a
63868 Großwallstadt
Germany

Fon: + 49 (0) 60 22 / 263 38 – 0
Fax: + 49 (0) 60 22 / 263 38 – 99
E-Mail: info@apsec.de
http://www.apsec.de

Bildnachweise:
Abbildung 1: © Ernst & Young/Statista
Abbildung 2 & 3: © Ponemon Institute/IBM
Abbildung 4: © apsec
Abbildung 5: © Evonik Industries AG

Management Summary:

Der Schutz sensibler Daten hat für Chemie- und Pharmaunternehmen herausragende Bedeutung. Datensicherheit ist fester Bestandteil verschiedenster Regularien, denen beide Branchen im Dienste der Qualitätssicherung verpflichtet sind. Gleichzeitig gilt es gerade in der chemischen und pharmazeutischen Industrie, Produkt-Rezepturen sowie Informationen zu Herstellungsverfahren vor unbefugtem Zugriff zu schützen – denn sie sind das Kapital dieser Unternehmen. Studien belegen, dass die Pharmabranche besonders leidet, wenn es zu Sicherheitsbrüchen kommt und Daten in unbefugte Hände geraten. Die Lösung: systematische Datenverschlüsselung. Mit der konsequenten Umsetzung können Manager ihre Unternehmen vor Industrie-Spionage schützen und gleichzeitig gesetzlich verpflichtende Compliance-Vorgaben erfüllen. So setzen gute Firmenkapitäne ihre Unternehmen auch in stürmischen Zeiten auf Kurs in ruhige Gewässer.

Einführung

Sicherheit ist in der chemischen und pharmazeutischen Industrie ein zentrales Thema. Es reicht von den Produktionsverfahren über die Logistik bis hin zur Gebäudetechnik. Unternehmen in diesen Branchen müssen eine Vielzahl von unterschiedlichen Sicherheitsauflagen und Vorschriften erfüllen, deren Einhaltung von Behörden akribisch kontrolliert wird.
Auch zur Sicherung ihrer IT-Systeme müssen die Betriebe regulatorische Anforderungen– wie EU Annex 11 oder GAMP 5 – erfüllen. Dagegen bleibt es ihnen weitgehend selbst überlassen, wie sie für System- und Datensicherheit in ihrer Organisation sorgen. Dabei gehören gerade Chemie- und Pharmaunternehmen zu den besonders sensiblen Branchen in Bezug auf Spionage und Datendiebstahl. Laut einer Studie der Prüfungs- und Beratungsgesellschaft Ernst & Young (Quelle: www.ey.com) standen Forschung und Entwicklung im Jahr 2013 mit 52 Prozent an der Spitze der Geschäftsbereiche, die in Deutschland besonders häufig von Datenklau betroffen waren.

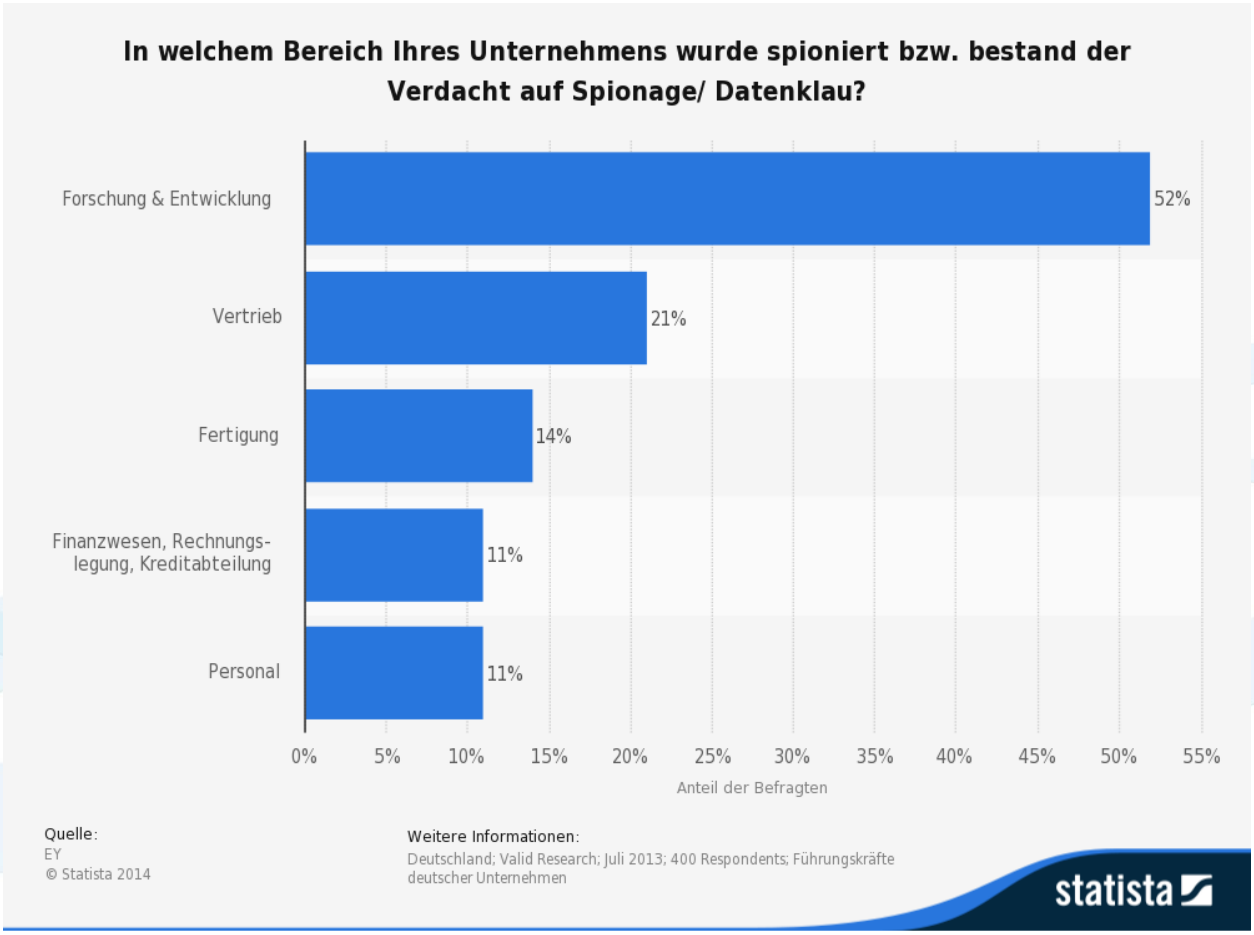

Abbildung 1: Forschung und Entwicklung sind am häufigsten von Datenklau und Spionage betroffen. Quelle: EY/Statista

Das wirtschaftliche Risiko ist enorm. Kosten entstehen Unternehmen dabei durch:

- Verlust von Patent- und Wettbewerbsvorteilen
- Kundenverluste aufgrund von Vertrauensverlust
- Kostenintensive Kampagnen zur Korrektur von Imageschäden
- Schadensersatzansprüche und Strafen

Gemäß der Studie **2014 Cost of Data Breach Study: Global Analysis** des amerikanischen Ponemon Intitutes beklagt die Pharmabranche am häufigsten Kundenverluste nach Datensicherheitsbrüchen.

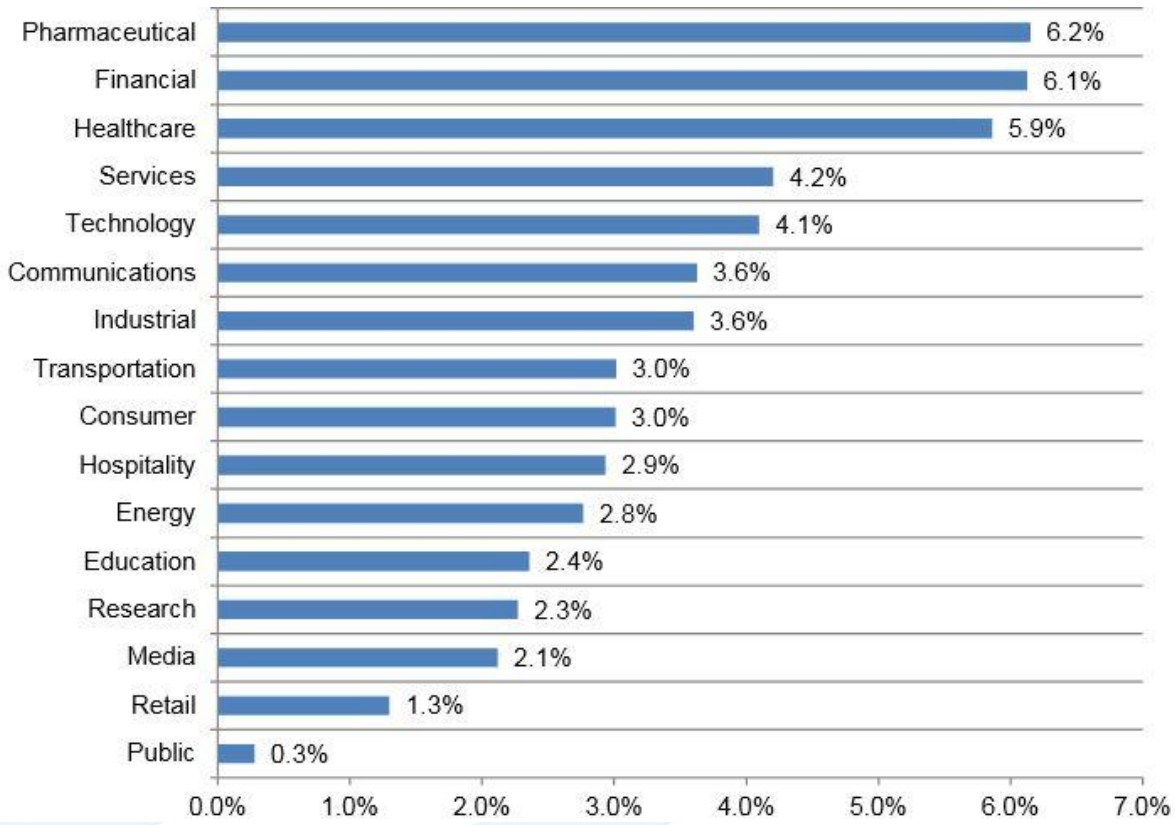

Abbildung 2: Kundenverluste nach IT-Sicherheitsvorfällen: am schlimmsten trifft es die Pharmabranche.
Quelle: 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute/IBM

Auch liegt die Pharmabranche nach der gleichen Studie weltweit auf Platz drei bei den durchschnittlichen Kosten, die pro Datensatz, der von einem Sicherheitsbruch betroffenen ist, entstehen. Da bei einem Sicherheitsvorfall in der Regel Hunderte oder eher sogar Tausende von Datensätzen betroffen sind, kumulieren sich die durchschnittlich 227$ pro Datensatz schnell zu großen Schadenssummen.

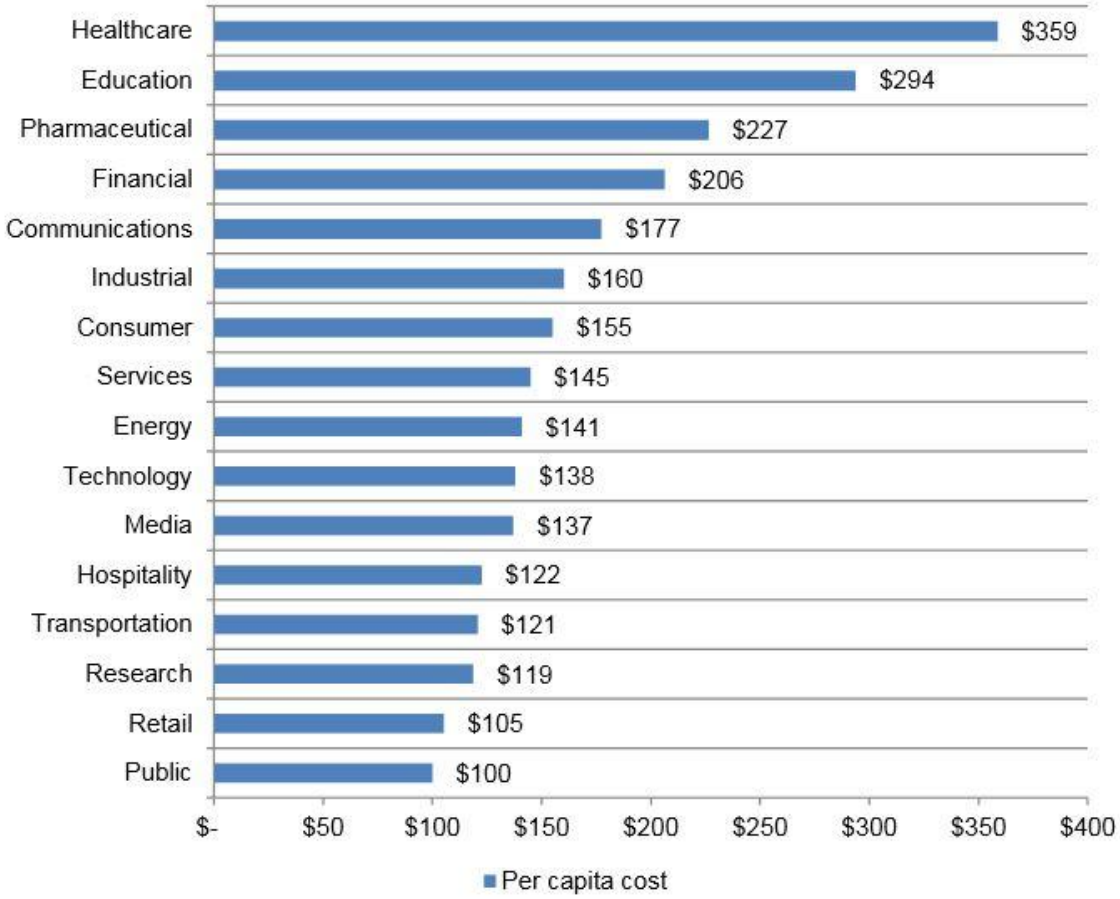

Abbildung 3: Durchschnittliche Kosten pro gestohlenem Datensatz.
Quelle: 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute/IBM

Nicht zu unterschätzen sind auch innerbetriebliche oder sogar juristische Konsequenzen, welche die Verantwortlichen bei zu nachlässigem Umgang mit den Risiken der Datenverarbeitung treffen können.

Um sich gegen einen unerwünschten Informationsabfluss zu schützen, greifen Unternehmen in der Regel noch zu scheinbar bewährten Methoden. Sie verlassen sich laut EY-Studie von 2013 hier vor allem auf den Schutz durch eine Firewall (85 Prozent) und den individuellen Passwortschutz (84 Prozent) auf den einzelnen Rechnern.

Dabei kann moderne Verschlüsselungssoftware eine deutlich zuverlässigere Lösung zum Schutz sensibler und vertraulicher Daten und Dokumente sein. Sie bieten die erforderliche Sicherheit bei zwei zentralen Handlungsfeldern von Unternehmen:

- beim Schutz des geistigen Eigentums
- beim Einhalten der Compliance-Regeln

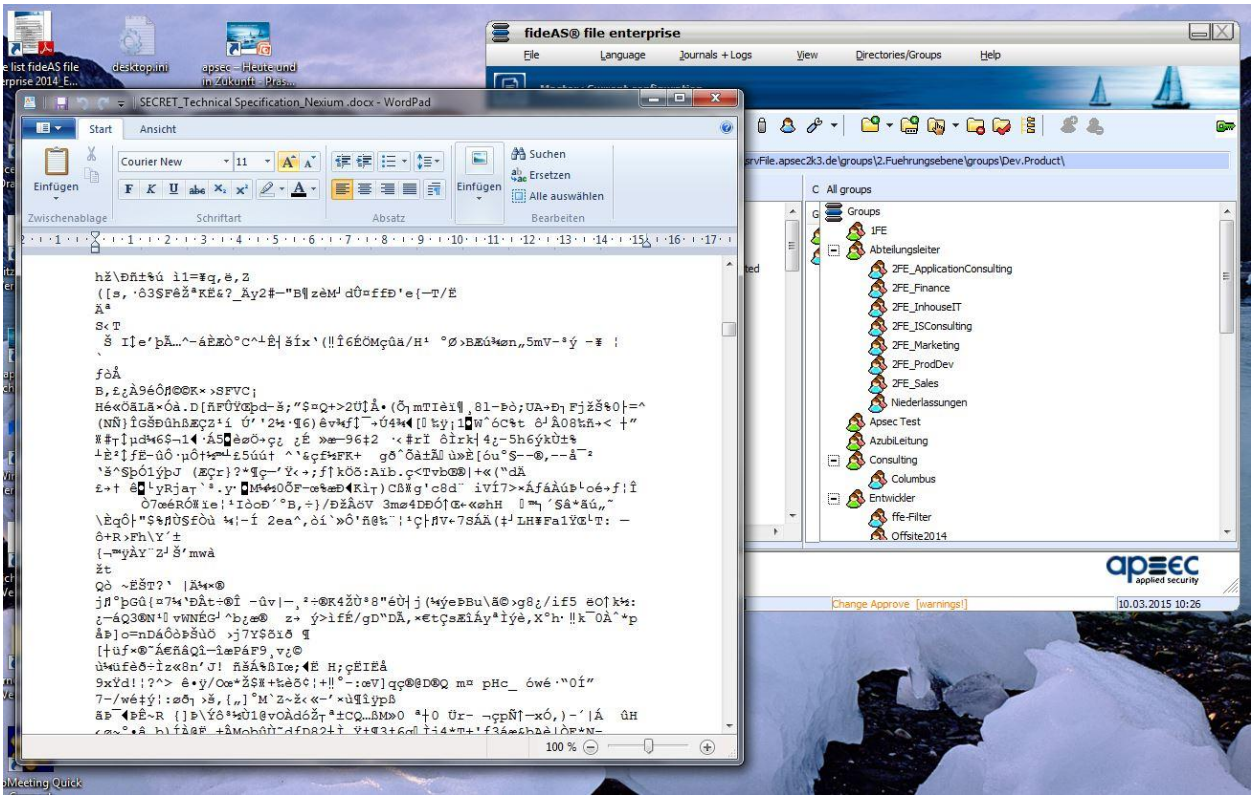

Abbildung 4: Verschlüsselte Dokumente sind für Datendiebe und Industriespione wertlos. Quelle: apsec

Schutz des geistigen Eigentums

Unternehmen der chemischen und pharmazeutischen Industrie sind darauf angewiesen, Informationen zu ihren Produkten geheim zu halten. Das gilt für Rezepturen ebenso wie für Herstellungsverfahren. Denn diese Betriebe investieren viel Zeit und Geld in die Entwicklung ihrer Produkte. Gerade in der Pharmabranche dauert es in der Regel mehrere Jahre, bis ein Präparat die Marktreife erlangt und zugelassen wird. Anschließend haben Hersteller nur ein begrenztes Zeitfenster, ihr Produkt zu vermarkten, bevor Wettbewerber sogenannte Generika – also Nachahmer-Präparate – auf den Markt bringen dürfen. In dieser Zeit müssen also Investitionskosten und Erträge erwirtschaftet werden.

Vor diesem Hintergrund bedarf es eines besonderen Schutzes für sensible Unternehmensdaten, um Produktpiraterie vorzubeugen und die eigene Wertschöpfungskette nicht zu gefährden. Eine systematische Verschlüsselung ist hierbei ein effektives Steuerungsinstrument, weil sie Zugriffsrechte genau definiert. Gerade bei großen Unternehmen, in denen abteilungs- und manchmal staatenübergreifend Daten und Informationen ausgetauscht werden, bleibt auf diese Weise immer kontrollierbar, wer zu welchem Zeitpunkt Zugang zu bestimmten Daten hat. Bedeutsam ist dies auch für den externen Datenaustausch: Speziell Firmen der Chemie- und Pharmabranche arbeiten mit einer Vielzahl von unterschiedlichen Dienstleistern und Behörden zusammen, denen sie oft wichtige Informationen zu ihren Anlagen und Produkten übermitteln. Durch eine sichere Verschlüsselung kann auch hier gewährleistet werden, dass Daten nicht in die falschen Hände gelangen.

Einhalten von Compliance-Vorschriften
Die Globalisierung und der damit einhergehende allgegenwärtige Einsatz von Informationstechnologie in Verwaltung und Fertigung haben zur Folge, dass Unternehmen zunehmend Sorgfaltspflichten erfüllen müssen. Im Bereich der Pharma-Industrie sind sie beispielsweise den Regularien der Europäischen Union (EU) und der US-Arzneimittelbehörde FDA unterworfen. Dies gilt auch für Chemiebetriebe, die die Anwendungsfelder ihrer Produkte auf medizinische oder pharmazeutische Bereiche ausweiten wollen.

Wer gegen die unterschiedlichen Compliance-Regeln verstößt, muss gemäß der Rechtsprechung in der Europäischen Union und der USA mit gravierenden Konsequenzen rechnen:

- Verlust der Marktzulassung
- Verpflichtung zu Rückrufaktionen, Schadensersatz und Produkthaftung
- Auflagen und Re-Audit nach einem Behördenaudit
- Verlust der Herstellerzulassung
- Verantwortliche können persönlich haftbar gemacht werden
- Geldstrafen
- Stilllegung des Betriebs

Im Sinne der Qualitätssicherung müssen Unternehmen also beispielsweise die Richtlinien des Medizinproduktgesetzes (MPG) oder des Good Manufacturing Practice (GMP) erfüllen. Beide sind für die Firmen bindend – Kontrolle erfolgt durch Behörden oder unabhängige Stellen – und haben eine gemeinsame Verpflichtung: Die komplette Infrastruktur eines Unternehmens, einschließlich Daten und Dokumente, muss durch intern beherrschte Methoden und Prozesse vor Manipulation geschützt sein.
Auch hier hilft die systematische Verschlüsselung von Daten und Dokumenten. Ein Berechtigungskonzept allein – wie es in zahlreichen Betrieben angewendet wird – stellt nicht sicher, dass Zugriffsrechte nicht missbraucht werden. Erst das Aufsetzen einer integrierten Lösung – wie etwa Verschlüsselung – kann verhindern, dass unbefugte Dritte auf Daten zugreifen, sie verändern oder entwenden können.
In Bezug auf Wirkstoffe sowie auf die Human- und Tiermedizin schreiben die Leitlinien der „Guten Herstellungspraxis“ beispielsweise eine genaue Dokumentation von Prozessen vor. Allein durch diese Anforderung entsteht eine große Anzahl sensibler Dokumente, die durch Verschlüsselung vor unbefugtem Zugriff geschützt werden müssen.

Praxisbeispiel aus der Branche: Evonik Industries AG
Die Evonik Industries AG macht vor, wie Informationen angemessen geschützt werden können, ohne dabei ihre Nutzer über Gebühr einzuschränken. Das Unternehmen setzt dafür eine Verschlüsselungssoftware der Applied Security GmbH (apsec) ein. Diese Lösung versetzt das Unternehmen in die Lage, die rechtlichen Vorschriften zum Datenschutz und andere Compliance-Regeln zu erfüllen und bildet somit einen wichtigen Baustein in der Wertschöpfungskette des erfolgreichen Konzerns. (Lesen Sie dazu mehr in einem Fachbeitrag auf www.chemanager-online.com)

Abbildung 5: Evonik Industries setzt auf Verschlüsselung Made in Germany.
Quelle: Evonik

Fazit:

Der Markt und das Umfeld, in dem sich Chemie- und Pharmaunternehmen bewegen, sind von zahlreichen Regularien geprägt. Gleichzeitig gehören beiden Branchen zu den Geschäftsbereichen, die in Deutschland am häufigsten zu Zielen von Industriespionage werden. Es liegen also eine Grundanforderung sowie eine wirtschaftliches Notwendigkeit vor, wirksame Maßnahmen zur Risikosteuerung und zum Schutz von Unternehmensdaten zu ergreifen. Gute Manager handeln entsprechend.

Über apsec

Die Applied Security GmbH (apsec) mit Sitz in Großwallstadt (Bayern) wurde 1998 gegründet und gehört zu den führenden deutschen Beratungshäusern und Softwareherstellern mit dem Fokus Informationssicherheit.
apsec ist spezialisiert auf die Themen sichere Datenübertragung und Verschlüsselung, sowie auf Informationssicherheits-Managementsysteme (ISMS).

Zu den Kunden der Verschlüsselungslösungen von apsec zählen unter anderem die Evonik Industries AG, der Deutsche Bundestag und die Landesbank Baden-Württemberg.

apsec ist Mitglied im Bundesverband der deutschen IT-Sicherheitswirtschaft Teletrust e.V, im BITKOM, im Cyber-Sicherheitsrat e.V, sowie Partner der Allianz für Cybersicherheit.

apsec ist berechtigt, das Qualitätssiegel **IT-Security Made in Germany** des Teletrust e.V. zu tragen.

apsec ist der Initiator der Initiative **Deutschland.Sicher.Jetzt** (www.deutschland-sicher-jetzt)

Ausführliche Informationen, Datenblätter, Anwenderberichte von Kunden und kostenlose Testversionen von Software befinden sich auf den apsec-Webseiten zu folgenden Themen:

Datei- und Ordnerverschlüsselung im LAN:	www.apsec.de/loesungen/fideas-file-enterprise/
Cloud-Verschlüsselung:	www.apsec.de/loesungen/fideas-cloud-services/
E-Mail-Verschlüsselung:	www.apsec.de/loesungen/fideas-mail/
Festplattenverschlüsselung:	www.apsec.de/loesungen/securedisk-bitlocker/
Datenbankverschlüsselung:	www.apsec.de/loesungen/eperi-datenbank-verschluesselung/

Fragen und Feedback zu diesem Whitepaper sind willkommen unter der E-Mail-Adresse marketing@apsec.de.