Schriftenreihe des Fachbereiches
Wirtschaftswissenschaften Sankt Augustin

Andreas Gadatsch

Auswirkungen veralteter Software, insbesondere spezieller Betriebssysteme, auf Jahresabschlusstestate

Band 34

Sankt Augustin, Dezember 2014

ISBN 3-938169-34-6

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Impressum

Hochschule Bonn-Rhein-Sieg
Fachbereich Wirtschaftswissenschaften Sankt Augustin
Grantham-Allee 20
53757 Sankt Augustin
Germany

Prof. Dr. Andreas Gadatsch
Tel.: +49 2241 -865 -129
Fax: +49 2241 -865 -8129
Email: andreas.gadatsch@h-brs.de

Schutzgebühr: € 50,-

Schriftenreihe des Fachbereiches Wirtschaftswissenschaften Sankt Augustin

herausgegeben von:

Fachbereich Wirtschaftswissenschaften Sankt Augustin
Hochschule Bonn-Rhein-Sieg
Grantham-Allee 20
53757 Sankt Augustin
Germany
Tel.: +49 2241 -865 -101
Fax: +49 2241 -865 -8101
Email: fb01.sekretariat@h-bonn-rhein-sieg.de
Internet: www.fb01.h-brs.de

ISBN 3-938169-34-6

Auswirkungen veralteter Software, insbesondere spezieller Betriebssysteme, auf Jahresabschlusstestate

Band 34

Andreas Gadatsch

Zusammenfassung

Unternehmen nutzen teilweise veraltete Betriebssystem-Software, die nicht mehr gewartet werden. Beispiele sind „Windows XP“ oder ab 14.05.2015 „Windows Server 2003“ der Firma Microsoft. Das Paper analysiert die Situation im Hinblick auf signifikante Risiken wie z. B. die mögliche Versagung von Jahresabschlusstestaten und schlägt Maßnahmen für das Management vor.

Summary

Companies often use operating systems which are partially outdated and out of maintenance. Current examples are ‘Windows XP’ and the server operating system ‘Windows Server 2013’ from Microsoft, which will expire on May 14th in 2015. This paper analyses the situation with regard to significant risks such as the potential withholding of approval of the annual financial statement. Furthermore the paper suggests actions for the management.

Inhaltsverzeichnis

Seite

Abkürzungsverzeichnis

AktG	Aktiengesetz
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIO	Chief Information Officer
ERP	Enterprise Resource Planning
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	GmbH-Gesetz
HGB	Handelsgesetzbuch
IT	Informationstechnik / Informationstechnologie

1 Problemstellung

In der betrieblichen Praxis wird teilweise Software genutzt, die keiner regelmäßigen Wartung durch den Softwarehersteller mehr unterliegt weil das Produkt das Ende seines Lebenszyklus erreicht hat. Dies umfasst neben Anwendungssoftware auch Betriebssysteme bzw. betriebssystemnahe Software. Aktuelle Beispiele sind die weit verbreiteten Produkte der Firma Microsoft, wie das bereits außerhalb der Wartung befindliche Betriebssystem „Windows XP" (Microsoft, 2014b), welches typischerweise als Client-Software zum Einsatz kam und nach wie vor noch von vielen Kunden genutzt wird (Redaktion ICT, 2014). Als jüngstes Beispiel ist das Serverbetriebssystem „Windows Server 2003" zu nennen für das am 14.05.2015 die Wartung beendet wird (Microsoft, 2014a).

Im Rahmen der Studie wird untersucht, welche Risiken und Konsequenzen der Einsatz veralteter (Betriebssystem-) Software auf das Informationsmanagement und IT-Controlling der Unternehmen hat und welche Handlungsempfehlungen hieraus abzuleiten sind. Insbesondere wird analysiert, wie sich nicht mehr gewartete Betriebssysteme auf die Erteilung von Jahresabschluss-Testaten deutscher Wirtschaftsprüfer auswirken könnte.

2 Methodik

Im Rahmen des Projektes erfolgte eine Literaturanalyse und Internetrecherche. Aufbauend auf diesen Ergebnissen wurde eine Erhebung bei deutschen Wirtschaftsprüfungsunternehmen in Form von strukturierten Interviews konzipiert und durchgeführt. Abschließend wurden Handlungsempfehlungen für Unternehmen abgeleitet. Die Untersuchung wurde in der Zeit zwischen dem 01.10.2014 und 30.11.2014 durchgeführt.

3 Analyse

3.1 Einführung in den Sachverhalt

Seit Beginn der betrieblichen Datenverarbeitung nutzen Anwender den Wartungsservice von Softwareherstellern, also die fachliche, rechtliche und technische Weiterentwicklung von Software. Üblicherweise wird Software von den Herstellern in Produktversionen (Releases) auf den Markt gebracht und für die Zeit des Verkaufs regelmäßig aktualisiert (Softwarewartung). Dies betrifft sowohl Betriebssysteme, als auch Anwendungssoftware (z.B. für Produktion, Logistik und Vertrieb).

Nach einiger Zeit der Nutzung ist es für Hersteller teilweise sinnvoll völlig neu entwickelte Produktversionen am Markt zu platzieren und die alten Produkte vom Markt zu nehmen, da diese sich nicht immer an aktuelle technologische Entwicklungen anpassen lassen. Für eine Übergangszeit werden die Altsysteme noch gewartet, so dass der Kunde die Möglichkeit hat, eine Migration auf das Nachfolgeprodukt des Herstellers oder Produkte anderer Hersteller zu planen. Nach Abschluss der Wartung bleibt das Softwareprodukt in seinem Zustand „eingefroren", wird also nicht mehr verändert.

Die Nutzung von Software nach Beendigung der Herstellerwartung kann je nach Softwareart und Einsatzzweck unterschiedliche Risiken und Konsequenzen haben.

3.2 Aktuelles Beispiel: „Microsoft Server 2003"

Die Firma Microsoft beendet am 14.05.2015 die Wartung für das weltweit verbreitete Betriebssystem „Microsoft Server 2003" (vgl. Microsoft, 2014a). Außerdem wird auch der Telefon-Support eingestellt (vgl. Microsoft 2014d). Hierbei handelt es sich um ein Softwaresystem, das speziell für Unternehmens-Server entwickelt wurde. Es stellt die Basis für zahlreiche betriebliche Aufgaben mit zum Teil geschäftsrelevanter Bedeutung dar. Beispiele hierfür sind der Betrieb von Servern für Internet-Services (http, smtp, pop3, u.a.), Dateiserver (Dokumentenmanagement), Applikationsserver (z.B. ERP-Systeme, Lagerwirtschaft, Buchhaltung) oder Druckserver.

Der Hersteller Microsoft versucht zur Umsetzung seiner Migrationsstrategie bereits seit etwa Juli 2014 mittels einer „Roadshow“ und weiterer Kampagnen seine Kunden dazu zu bewegen auf Nachfolgeprodukte zu migrieren (vgl. Microsoft, 2014c). Microsoft weist z.B. auf seiner OEM-Partnerwebseite offiziell darauf hin, dass die Systeme von Unternehmen mit Kreditkartenverkehr nach dem Wartungsende nicht mit den Datensicherheitsstandards der Payment Card Industry (PCI) konform sind und damit die Zusammenarbeit mit den Kreditkartenanbietern Visa und Mastercard nicht mehr sicher gewährleistet werden kann (vgl. Microsoft, 2014d). Diese Thematik wurde in verschiedenen Blogs der IT-Branche bereits aufgegriffen und thematisiert (z. B. Young, 2014; Wassong, 2014). Offen ist, ob alle Kunden hierauf migrieren können und wollen. Es besteht sicherlich Grund zur Annahme, dass einige Anwender keine Migration durchführen und das eingefrorene System noch weiter nutzen, um die erforderlichen Investitionen zu vermeiden.

4 Auswirkungen für die Unternehmen

4.1 Technische Perspektive

4.1.1 Problemlage

Nach dem Ende der Wartungsphase wird der Softwarehersteller keine „Updates“ oder „Security-Patches“ mehr an seine Kunden ausliefern. Die Software wird durch diese Situation „verwundbar“, d.h. es muss jederzeit mit einem Angriff gerechnet werden, dessen Angriffsziel der durch die Verwundbarkeit offen gelegte Angriffspunkt (hier: fehlende Wartung) ist (vgl. Knoll, 2014, S. 39). Insbesondere können bekannte oder neu identifizierte Schwachstellen des Systems, die nicht mehr durch Wartungsmaßnahmen ausgeglichen werden, durch Dritte (Hackerangriff, Virenangriff, u.a.) genutzt werden, um in die Systeme einzudringen, Daten zu lesen, zu kopieren, zu verändern oder zu löschen.

Der Betrieb neuerer Anwendungs-Software könnte zudem Kompatibilitätsprobleme verursachen, d.h. es wäre denkbar, dass neuere Anwendungssoftware nicht mehr mit dem alten Betriebssystem genutzt werden kann.

Durch den fehlenden Support ist es daher für Drittanbieter uninteressant, Applikationen für veraltete Betriebssysteme zu entwickeln. Insgesamt sind höhere Systemausfallzeiten und Wartungskosten zu erwarten.

4.1.2 Notwendigkeit zum Upgrade und Migration

Angesichts der o.g. Problemlage stellt sich die Frage, ob es einen Zwang zum „Update" auf Nachfolgeprodukte des gleichen Herstellers oder eine „Migration" auf neue Produkte anderer Hersteller gibt. Die Frage kann verneint werden: Es ist in Deutschland nicht gesetzlich vorgeschrieben, dass Unternehmen die jeweils aktuellste Software einsetzen müssen (vgl. Orthwein, 2014). Einen Zwang zum „Upgrade" gibt es weder innerhalb regulär gewarteter Software, noch einen Zwang zur „Migration" vom Vorgänger zum jeweiligen Nachfolgerprodukt. Allerdings müssen Unternehmen nach betriebswirtschaftlichen Grundsätzen verantwortlich handeln und die jeweils für Sie relevanten Datenschutzbestimmungen und Regelungen zur IT-Sicherheit beachten (vgl. Orthwein, 2014). Die Verantwortung für die Sicherheit der Daten kann auch im Fall der „Auftragsdatenverarbeitung" (IT-Outsourcing) durch Dritte nicht verlagert werden (vgl. §11 BDSG und IDW 2002, S. 21).

4.1.3 Konsequenzen

Unternehmen sollten Ihre IT-Strategie auf Ihre Belange anpassen, um die individuellen Sicherheitsanforderungen zu erfüllen. Mögliche Sicherheitsanforderungen und notwendigen Maßnahmen werden bei einer Bank, einer Versicherung oder einer Behörde sicherlich anders ausfallen, als bei einem lokal tätigen Handelsunternehmen für nicht gefährliche alltägliche Gebrauchsgüter. Hohe Sicherheitsanforderungen können dazu führen, dass bei sicherheitsrelevanten Fragen der jeweilige aktuelle Stand der Technik im Rahmen der Unternehmensstrategie zu berücksichtigen ist (vgl. Orthwein 2014). Dies könnte bedeuten, dass ein Unternehmen faktisch gezwungen ist, ein veraltetes Betriebssystem abzulösen, um personenbezogene Daten zu schützen. Das Bundesdatenschutzgesetz (BDSG) verlangt schützenswerte Daten in geeigneter Form vor Weitergabe, Manipulation und unzulässige Nutzung zu verarbeiten. Allerdings müssen die notwendigen Maßnahmen auch wirtschaftlich vertretbar sein (vgl. Orthwein 2014).

Text des § 9 BDSG: „Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht." Bei Verstößen können hohe Bußgelder oder bei Vorsatz auch Geld- oder Freiheitsstrafen verhängt werden. Daneben sind Schadensersatzansprüche Dritter denkbar."

Sofern für die Verantwortlichen erkennbar ist, dass die eingesetzte Software nicht in der Lage ist, die Anforderungen zu erfüllen, kann auch „Nichthandeln" fahrlässig oder sogar grob fahrlässig sein (vgl. Orthwein, 2014).

4.2 Betriebswirtschaftliche Perspektive

4.2.1 Problemlage

Der Software-Kunde ist hohen Sicherheits- und Compliance Risiken ausgesetzt, die umso größer werden, je länger Software-Anwendungen auf der Basis eines veralteten und eingefrorenen Betriebssystems betrieben werden. Jedes nicht regelmäßig aktualisierte Betriebssystem birgt letztlich die Gefahr, dass Sicherheitslücken entstehen oder entdeckt werden, die zu nicht erlaubten Maßnahmen durch Dritte führen können.

Der Gesetzgeber schreibt zwar nicht vor, dass regelmäßig Updates von Betriebssystemen oder Anwendungssoftware u. ä. durchzuführen sind, aber die Unternehmen müssen die allgemeinen gesetzlichen Anforderungen erfüllen und sich durch geeignete Technologien entsprechend vor vermeidbaren Gefahren schützen.

Laufen auf dem veralteten Betriebssystem beispielsweise geschäftsrelevante Anwendungen (z.B. ERP-System, Buchhaltung, Lagerwirtschaft) die für den Jahresabschluss relevante Daten erzeugen, besteht u.a. die Gefahr der Verfälschung des Jahresabschlusses oder die Gefahr, dass nach den Datenschutzgesetzen zu schützende Daten oder Geschäftsgeheimnisse verloren gehen.

Somit sind aus betriebswirtschaftlicher Sicht folgende Aspekte zu beachten, wenn veraltete Betriebssysteme weiter genutzt werden:

- Kompatibilitätsprobleme beim Einsatz neuer Applikationen auf dem veralteten Betriebssystem,
- Imageschäden durch negative Außendarstellung bei Datenverlusten oder Datenmanipulationen,
- Vermögensschäden durch Verlust von Aufträgen (wenn z.B. Aufträge durch Bekanntgabe von Angebotsinhalten verloren gehen),
- Schadensersatzansprüche Dritter bei Verstoß gegen Datenschutzgesetze (wenn z.B. schützenswerte Informationen nach außen gelangen).

4.2.2 Auswirkungen auf die Gültigkeit des Jahresabschlusstestats

Unter bestimmten Voraussetzungen sind Unternehmen verpflichtet Ihren Jahresabschluss zu veröffentlichen und durch Wirtschaftsprüfer einer Jahresabschlussprüfung zu unterziehen, bei der die Ordnungsmäßigkeit der Buchführung untersucht wird. Im Rahmen der Jahresabschlussprüfung erfolgt eine IT-Systemprüfung, bei der vom Wirtschaftsprüfer versucht wird Fehlerrisiken in IT-Systemen zu identifizieren (vgl. IDW-RS-FAIT-1 2002 und IDW PS 330).

Die IT-Systemprüfung ist sehr breit angelegt und umfasst die IT-Strategie, IT-Umfeld, IT-Organisation, IT-Infrastruktur, IT-Anwendungen und IT-Prozesse sowie ggf. das IT-Outsourcing (Freidank et al., 2007, S. 733, Stichwort IT-Systemprüfung). Die IT-Systemprüfung umfasst u.a. die Beurteilung der internen Kontrollsysteme und Geschäftsprozesse sowie organisatorischer und technischer Sicherungen (vgl. Hasenkamp und Kozlova, 2009).

Die Abschlussprüfer erteilen im Rahmen der Jahresabschlussprüfung einen Bestätigungsvermerk (Testat) nach § 322 I 3 HGB. Hierbei können Einwendungen (geringfügige Beanstandungen) und / oder Einschränkungen geltend gemacht werden.

Ebenso ist eine Versagung des Bestätigungsvermerkes denkbar, was zur Ungültigkeit des Jahresabschlusses führt, dem sogenannten „Versagungsvermerk" (Gabler, 2014, Stichwort „Bestätigungsvermerk"). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist ebenfalls in seinem „IT-Grundschutzkatalog" unter der Rubrik „Gefährdungskatalog Elementare Gefährdungen" darauf hin, dass bei unsachgemäßem Umgang mit der Elektronischen Datenverarbeitung (EDV) und gravierenden Sachmängeln das Jahresabschlusstestat verweigert werden kann (BSI, 2014, G029, S. 29).

Die Einschränkung oder die Versagung des Bestätigungsvermerkes kommt in der Praxis zwar vor, ist aber relativ selten, wie eine Auswertung der Wirtschaftsprüferkammer (2010) zeigt. Noch viel seltener ist die Versagung des Vermerkes im Zusammenhang mit ungeeigneter Informationstechnik. Im 139 Seiten starken Bericht, der Textstellen mit Formulierungen zu versagten bzw. eingeschränkten Testaten umfasst, tauchen die Begriffe „Windows", „XP", „EDV", „IT", „Informationstechnik" überhaupt nicht auf. Lediglich die Suche nach „System" führte zu einer Textstelle mit Bezug zur IT-orientierten Einschränkung eines Testates. Sie betraf die fehlende Verfügbarkeit eines Warenwirtschaftssystems (Wirtschaftsprüferkammer 2010, S. 7) und der damit verbundenen Unmöglichkeit, die Eröffnungsbilanzsumme zu bestimmen.

4.3 Verantwortlichkeit für die Aktualität von Informationssystemen

Die Aktualisierung von Informationssystemen ist unter dem Gesichtspunkt des Datenschutzes und der IT-Sicherheit zu betrachten. Die Verantwortung für die IT-Sicherheit ist nicht nur eine Aufgabe des IT-Leiters, sondern auch in der Verantwortung der Unternehmensleitung. Dies ergibt sich aus den Vorschriften der Gesetze für Körperschaften (§91 Abs. 2 AktG und § 43 Abs. 1 GmbHG). Hierbei werden die Anforderungen an die Unternehmensführung eines sorgfältigen Kaufmanns zugrunde gelegt.

Die Situation wird noch durch die vielfach anzutreffende sogenannte „Schatten-IT" verschärft. Hierunter sind von Anwendern entwickelte Applikationen zu verstehen, die nicht unter der Federführung und Kontrolle der IT-Verantwortlichen stehen und „inoffiziell" betrieben werden. Dies wiederum könnte dazu führen, dass evtl. veraltete Serverbetriebssysteme nicht migriert werden, damit das „Schatten-System" nicht auffällt.

5 Validierung der Analyse

5.1 Erhebung unter ausgewählten Wirtschaftsprüfern

5.1.1 Fragen an die Wirtschaftsprüfer

Zur Validierung der o.g. Ergebnisse wird die Erhebung der Wirtschaftsprüfungspraxis als sinnvoll erachtet. Zu diesem Zweck wurden einige Wirtschaftsprüfungsgesellschaften ohne Anspruch auf Vollständigkeit oder qualitative Wertung ausgewählt und per Email kontaktiert. Mit den ausgewählten Gesellschaften sollten mündliche Kurzinterviews anhand eines strukturierten Fragebogens durchgeführt werden, der den Teilnehmern vorab zugesandt wurde.

Der den Gesellschaften übersandte Fragebogen enthielt folgende Fragen:

1. Welche Auswirkung hat der Betrieb von Servern mit dem Betriebssystem Microsoft Windows 2003 nach August 2015 (Ende der Wartung) in Bezug auf Wirtschaftsprüfungsrelevante Belange wie z.B. Datenverarbeitung, -vorhaltung, -speicherung, -sicherheit und Recovery?
2. Welche Konsequenzen leiten Sie als Wirtschaftsprüfer ab, wenn Sie im Rahmen ihrer Prüfungsaufgaben auf Serversysteme stoßen, die mit einem Betriebssystem arbeiten, das keinen Herstellersupport mehr hat?
3. Welche Auswirkungen haben Komplikationen, die durch Systeme mit veralteten Betriebssystemen hervorgerufen werden auf die Unternehmensleitung (insbesondere CEO, CFO, CIO)?
4. Wie unterscheiden sich die Auswirkungen für kleinere, mittelständische und Großunternehmen?
5. Welche Lösungen gibt es auf dem Markt, die ein Unternehmen implementieren kann, um das Risiko zu minimieren?
6. Ist es aus Ihrer Perspektive sinnvoll, die Analyse europaweit fortzuführen?

Insgesamt wurden sechs Gesellschaften kontaktiert. Davon haben vier Gesellschaften verwertbare Informationen geliefert, deren Umfang und Detaillierung allerdings stark variiert. Zudem wurde nicht immer direkt auf die einzelnen Fragen geantwortet, sondern allgemein argumentiert.

5.1.2 WP-Gesellschaft A

Eine lokal begrenzt tätige Wirtschaftsprüfungsgesellschaft mit einem Kundenkreis im Umfeld kleinerer und mittlerer Unternehmen sieht in der Praxis kein Problem. Sie betreut einen sehr weit gestreuten Mandantenkreis. Man ist der Auffassung, dass es faktisch kein Problem gibt, „weil die großen und mittleren Unternehmen regelmäßig ihre EDV up to date halten und die kleinen Gesellschaften oftmals nicht prüfungspflichtig sind." Praktische Erfahrungen anhand konkreter Fälle liegen nicht vor.

5.1.3 WP-Gesellschaft B

Eine international ausgerichtete Wirtschaftsprüfungsgesellschaft ist der Auffassung, dass nur besonders eklatante Aspekte einer IT-Systemprüfung für den Abschlussprüfer interessant sind. Aspekte der Informationsverarbeitung werden daher in Abschlussberichten nur selten erwähnt, es sei denn, es liegen gravierende Mängel vor. Eine Versagung des Bestätigungsvermerkes ist demnach nur dann denkbar, wenn vom IT-Prüfer dargelegt werden kann, dass aufgrund fehlender Verlässlichkeit der Daten wesentliche Teile der Rechnungslegung nicht mehr mit hinreichender Sicherheit beurteilt werden können.

5.1.4 WP-Gesellschaft C

Eine weitere international tätige Gesellschaft stellt fest, dass der Prüfungsauftrag des Wirtschaftsprüfers weniger stark in der Zukunft, als in der Vergangenheit liegt. Es wird ein Jahresabschluss der sich auf das abgelaufene Geschäftsjahr bezieht geprüft, also die Abbildung der Vergangenheit. Aus dieser Perspektive ist ein Unternehmen, das ein bereits veraltetes Betriebssystem wie „Windows XP" einsetzt, anders zu beurteilen, als ein Unternehmen, dass im nächsten Jahr möglicherweise ein veraltetes System nutzt. IT-Systemprüfungen werden generell durchgeführt. Bei Verdacht auf Schwachstellen (z.B. ein veraltetes System) oder festgestellten Fehlern im Jahresabschluss (z. B. fehlerhafte Kontensalden) werden verstärkt Stichproben der relevanten Geschäftsvorfälle analysiert. Dies geschieht aber ohnehin völlig unabhängig von IT-Fragen, insbesondere wenn Verdachtsmomente hinsichtlich Betrugs vorhanden sind. Schwachstellen im internen Kontrollsystem können aber dazu führen, dass dies zu Hinweisen auf die Ver-

letzung der allgemeinen Sorgfaltspflichten nach dem Aktiengesetz führen kann. Eine Versagung oder Einschränkung des Testats ist allerdings in der Praxis nur in extremen sehr seltenen Ausnahmefällen zu erwarten.

5.1.5 WP-Gesellschaft D

Eine andere international tätige Gesellschaft machte sich die Mühe, den vorgestellten Fragenkatalog ausführlich zu beantworten. Nachfolgend sind die Antworten (kursiv) aufgeführt.

1. Welche Auswirkung hat der Betrieb von Servern mit dem Betriebssystem Microsoft Windows 2003 nach August 2015 (Ende der Wartung) in Bezug auf Wirtschaftsprüfungsrelevante Belange wie z.B. Datenverarbeitung, -vorhaltung, -speicherung, -sicherheit und Recovery?

   Grundsätzlich hat der Ablauf einer Betriebsversion (hier Microsoft Windows 2003) unserer Meinung nach drei wesentliche Auswirkungen:
   a.) Auftretende Sicherheitslücken auf Betriebssystemebene werden nicht mehr geschlossen.
   b.) Die Kompatibilität von „neuer" Anwendungssoftware ist nicht mehr zweifelsfrei gegeben. Es kann hierdurch zu einem erhöhten Fehlerrisiko, insbesondere in den Bereichen ERP und Datenbanken kommen.
   c.) Das Auslassen von Versionen führt zu einer fehlenden direkten Updatefähigkeit und damit einhergehenden exponentiell steigenden Updatekosten. Er kann dadurch zu einem erhöhten Risiko bspw. bzgl. des Lageberichts kommen.

2. Welche Konsequenzen leiten Sie als Wirtschaftsprüfer ab, wenn Sie im Rahmen ihrer Prüfungsaufgaben auf Serversysteme stoßen, die mit einem Betriebssystem arbeiten, das keinen Herstellersupport mehr hat?

   Erhöhte Risiken, wie wir diese in der Beantwortung der Fragestellung ad 1. aufgeführt haben, führen in der Regel zu einer Erhöhung der analytischen und insbesondere der substanziellen Prüfungsbedingungen (extensive Ausweitung der Belegprüfung bzgl. der Manipulation von Daten bzw. Datenverlust sowie möglicher Fehler in den Anwendungssystemen des ERP).
   Darüber hinaus können sich Berichtspflichten im Lagebericht der zu prüfenden Gesellschaft sowie eine Redepflicht im Prüfungsbericht zu den Ausführungen zum Datenverarbeitungssystem ergeben. Bei festgestellten Fehlern bzw. Datenverlust/-manipulation können sich auch im Extremfall Auswirkungen auf den Bestätigungsvermerk ergeben.

3. Welche Auswirkungen haben Komplikationen, die durch Systeme mit veralteten Betriebssystemen hervorgerufen werden auf die Unternehmensleitung (insbesondere CEO, CFO, CIO)?

   Gegebenenfalls können sich die Komplikationen, die durch Systeme mit veralteten Betriebssystemen hervorgerufen werden, derart auswirken, dass keine ausreichende IT-Governance mehr gegeben ist. Möglicherweise ergeben sich daraus Haftungsrisiken für die Geschäftsleitung aufgrund auftretender Vermögensschädigungen.

4. Wie unterscheiden sich die Auswirkungen für kleinere, mittelständische und Großunternehmen?

   Die Integration und Abhängigkeit von der Systemlandschaft ist aus unserer Sicht der entscheidende Risikofaktor. Generell ist allerdings zu erwarten, dass das Risiko für Großunternehmen mit hoher Komplexität exponentiell höher ist, als für Unternehmen kleiner Größe. Entscheidend ist hier jedoch die Komplexität des Unternehmens und weniger die Größe.

5. Welche Lösungen gibt es auf dem Markt, die ein Unternehmen implementieren kann, um das Risiko zu minimieren?

   Die Risikosituation kann sehr deutlich unseres Erachtens verbessert werden durch

   a.) Regelmäßige Updates

   b.) Einkauf von Sonderwartung durch den Hersteller

   c.) Einführung erhöhter Sicherheitsmaßnahmen (bspw. Penetrationstests) und eine häufige Durchführung von Anwendungstests

   d.) Anwendung des Continuous Monitoring Tools (Anwendungssicht).

6. Ist es aus Ihrer Perspektive sinnvoll, die Analyse europaweit fortzuführen

   Wir glauben, dass eine europaweite Analyse zielführend wäre. Wir merken aber auch an, dass eine intensivere Beleuchtung der Wirkung veralteter An-

wendungssoftware zielführend sein kann. Wir basieren unsere Meinung insbesondere auf der Argumentationskette, dass ein fehlendes Update des Betriebssystems oftmals fehlende Updates des ERP-Systems nach sich zieht und hierdurch kausal ein Investitionsstau generiert wird. Wir möchten hier als Beispiel die Otto-Gruppe anführen, die aktuell nach zwei gescheiterten Versuchen die veraltete Anwendungssoftware bei exponentiell erhöhten Kosten (mehr als 500 Mio. Euro) und verbunden mit erheblichen Risiken aktualisiert.

5.2 Schlussfolgerungen

Aus der durchgeführten Analyse kann abgeleitet werden, dass sowohl die Wirtschaftsprüfungsgesellschaften, als auch die betroffenen Unternehmen die Problematik als nicht sonderlich praxisrelevant einstufen, möglicherweise auch in seiner Wirkung unterschätzen.

Die Wirtschaftsprüfungsgesellschaften konzentrieren sich naturgemäß auf die inhaltliche Jahresabschlussprüfung. IT-Fragen und hieraus resultierende Risiken spielen hier neben inhaltlichen Fragen nur eine untergeordnete Rolle. Erst bei konkreten Verstößen bzw. Verdacht von Verstößen gegen relevante Vorschriften ist die Thematik „veraltete Betriebssysteme bzw. Anwendungssoftware“ für Wirtschaftsprüfer von Bedeutung. In diesem Fall führt dies zu einem höheren Untersuchungsaufwand, d.h. es werden mehr abschlussrelevante Belege geprüft.

Allerdings gibt es auch Wirtschaftsprüfer, die den Sachverhalt etwas kritischer sehen (hier WP-Gesellschaft „D“) und die möglichen Risiken stärker einschätzen, so insbesondere eventuelle Haftungsrisiken für die Geschäftsleitung. Auswirkungen auf den Bestätigungsvermerk (Testat) sind jedoch extrem selten.

Die betroffenen Unternehmen verkennen möglichweise den Zusammenhang zwischen fehlender Vorsorge in aktuelle Betriebssystemen und hieraus resultierenden Risiken. Vor diesem Hintergrund ist davon auszugehen, dass die auslaufende Wartung für die eingangs erwähnten Betriebssysteme nicht dazu führen wird, dass in großer Anzahl

Jahresabschlussprüfungen nicht testiert oder eingeschränkt werden. In kleineren Unternehmen liegt zudem oftmals keine Prüfungspflicht vor. Dennoch verbleibt für die Verantwortlichen in den Unternehmen ein Restrisiko, für das sie die Verantwortung übernehmen müssen.

6 Handlungsempfehlungen für Entscheidungsträger

Die Risiken durch die Weiternutzung nicht mehr gewarteter Software sind für die Unternehmen erheblich. Das Risiko einer Testat-Einschränkung oder gar Testat-Verweigerung ist eher gering.

Nachfolgend sind die zentralen Risiken zusammengefasst, für die Vorsorge zu treffen ist:

- der Kunde erhält keine „Updates“ oder „Security-Patches“ mehr,
- die Software wird fachlich, rechtlich und technisch „eingefroren“,
- Schwachstellen können durch Dritte genutzt werden, um in die Systeme einzudringen, Daten zu lesen, zu kopieren, zu verändern oder zu löschen,
- der Betrieb neuerer Anwendungen könnte aufgrund von Kompatibilitätsproblemen nicht möglich sein,
- Entkopplung vom technischen Fortschritt, da es für Drittanbieter uninteressant ist neue Applikationen für veraltete Betriebssysteme zu entwickeln .
- Höhere Systemausfallzeiten und Wartungskosten zu erwarten.

Die aufgeführten Risiken müssen im Rahmen der IT-Strategie des Unternehmens durch geeignete Ziele und Maßnahmen reduziert bzw. vermieden werden. „IT-Risiken zu ignorieren ist die schlechteste aller IT-Risikostrategien. Eine solche Strategie sollte niemals angewandt werden.“ (Knoll, 2014, S. 63).

Folgende Maßnahmen sind notwendig:

- Inventur der vorhandenen Software in Bezug auf Aktualität und regelmäßige Wartung,
- Identifizierung auslaufender Wartungsverträge bei Betriebssystemen und ggf. Anwendungssoftware
- Ermittlung eines „Business-Cases" für eine mögliche Migration auf Nachfolgeprodukte unter Einbeziehung der Kosten, Risiken und Nutzenaspekte
- Erarbeitung einer Strategie, welche die Sicherheitsbelange des Unternehmens widerspiegelt.

7 Fazit

Die identifizierten Risiken können von den betroffenen Unternehmen nicht ignoriert werden. Als Worst-Case-Szenario sind wie aufgeführt Datenverluste, Image-Schäden, Betriebsstörungen oder auch längere Stillstände denkbar. Mögliche Haftungsrisiken sind für die Geschäftsleitung in extremen Situationen denkbar.

Diese Szenarien sollten den Verantwortlichen bewusst sein, auch wenn vermutlichen in vielen Fällen keinerlei Schäden bekannt werden. Im Zweifel sollten keine nicht mehr gewarteten Betriebssysteme oder Anwendungssoftware genutzt werden und eine rasche Migration zu einer neueren Betriebssystemsoftware gewählt werden.

Literaturverzeichnis

BDSG Bundesdatenschutzgesetz, Online im Internet, http://www.gesetze-im-internet.de/bdsg_1990/__11.html, Abruf am 16.10.2014

BSI (Hrsg.): IT-Grundschutzkatalog, Gefährdungskatalog Elementare Gefährdungen, Verstoß gegen Gesetze oder Regelungen G029, 12. Ergänzungslieferung, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Download/download_node.html, Abruf 05.11.2014

Freidank, C.-C.; Lachnit, L.; Tesch, J.: Vahlens Großes Auditing Lexikon, München, 2007

Gabler Verlag (Hrsg.): Gabler Wirtschaftslexikon, Wiesbaden, Online im Internet http://wirtschaftslexikon.gabler.de/Archiv/54562/bestaetigungsvermerk-v10.html, Abruf am 16.10.2014

Gadatsch, A.; Mayer, E.: Masterkurs IT-Controlling, 4. Auflage, Wiesbaden, 2010

Hasenkamp, U.; Kozlova, E.: IT-Systemprüfungen, in: WISU, 01/2009, WISU-Studienblatt

IDW-RS-FAIT-: IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW
RS FAIT 1) (Stand: 24.09.2002)

IDW PS 330: Abschlussprüfung bei Einsatz von Informationstechnologie" (IDW PS 330), Institut der Wirtschaftsprüfer e. V.; www.idw.de, o.J.

Knoll, M.: Praxisorientiertes IT-Risikomanagement, Heidelberg, 2014

Microsoft (Hrsg.): Microsoft Hilfe und Support, Microsoft Product Lifecycle, 2014a, http://support2.microsoft.com/lifecycle/search/default.aspx?alpha=Windows+Server+2003+R2, Abruf am 30.10.2014

Microsoft (Hrsg.): Windows, Windows XP, 2014b, http://windows.microsoft.com/de-de/windows/lifecycle, Abruf am 30.10.2014

Microsoft (Hrsg.): Goodbye Windows Server 2003: kostenlose Update-Roadshow mit Microsoft-Experten, 2014c, http://www.microsoft.com/germany/ technet/ aktuell/ news/ show.aspx?id=msdn_de_55349, Abruf am 30.10.2014

Microsoft (Hrsg.): Microsoft OEM Partnercenter, 2014d http://www.microsoft.com/OEM/de/products/servers/Pages/windows-server-2012-sell.aspx#fbid=kDJiv_8u9H5, Abruf am 03.11.2014

Orthwein, M.: Windows XP Support Ende – Welche rechtlichen Pflichten folgen daraus für Geschäftsführer, IT Leiter und Reseller?, Webinar, 25.06.2014

Redaktion ICT: Windows XP verliert erstmals deutlich an Boden, in ICT, 03.11.2014, http://ictk.ch/content/windows-xp-verliert-erstmals-deutlich-boden Abruf am 03.11.2014

Wasson, A.: Payment Cards At Risk With End Of Support For Windows 2003, in: techsupport pro, 12.09.2014, http://techsupportwindows.com/windows-online-support-2/payment-cards-at-risk-with-end-of-support-for-windows-2003/, Abruf am 03.11.2014

Wirtschaftsprüferkammer (Hrsg.): Zusammenstellung der eingeschränkten oder ergänzten Bestätigungsvermerke für das Jahr 2010 (Anlage zum Bericht der Wirtschaftsprüferkammer zur Berufsaufsicht im Jahr 2010, Teil Abschlussdurchsicht), online im Internet http://www.wpk.de/ pdf/WPK_Berufsaufsicht_2010_ Bestaetigungsvermerke.pdf, Abruf am 30.10.2014

Young, D.: Businesses using Windows Server 2003 could face Visa & MasterCard Backlash, in: ebuyer.com, 14.06.2014, http://www.ebuyer.com/blog/2014/07/businesses-using-windows-2003-could-face-visa-mastercard-backlash/, Abruf am 03.11.2014