Bedingungen für das Lesen dieser Stellungnahme

Die AWADO GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft, Neu-Isenburg, hat im Auftrag der CORONIC GmbH, Kiel, den Einsatz des Browsers PROTECT in einer Bank beurteilt. Das Ergebnis ist die Stellungnahme vom 15. Oktober 2020 auf den folgenden Seiten. CORONIC stellt sie Banken und deren Prüfern zur Verfügung. Lesen Sie die Stellungnahme nur, wenn Sie diese fünf Bedingungen annehmen.

1. Grundlage der Stellungnahme ist der Auftrag zwischen CORONIC und der AWADO. Für ihn gelten die Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 1. Januar 2017. Mit dem Lesen erkennen Sie diese Auftragsbedingungen an. CORONIC stellt sie Ihnen auf Anfrage zur Verfügung.

2. Die Stellungnahme gibt den Stand vom Oktober 2020 wieder und wird nicht aktualisiert. Sie beruht auf Unterlagen und Auskünften von CORONIC. Was für Ihre Entscheidung wichtig ist, prüfen Sie selbst.

3. Die Stellungnahme ist vertraulich. Sie geben sie nicht an Dritte weiter. Ausgenommen ist eine Weitergabe, zu der ein Gesetz, ein Gericht oder eine Aufsichtsbehörde Sie verpflichtet.

4. Zwischen Ihnen und der AWADO entsteht kein Vertrag. Aus dem Auftrag zwischen CORONIC und der AWADO können Sie keine Rechte herleiten. Die AWADO haftet Ihnen gegenüber nicht, soweit das Gesetz das zulässt.

5. Es gilt deutsches Recht.

Ich nehme die Bedingungen an und öffne die Stellungnahme

Fachliche Stellungnahme der AWADO GmbH

Bescheinigung für den Einsatz des Protect Browsers in einer Bank für den Hersteller

CORONIC GmbH
Schauenburgstraße 116
24118 Kiel

vom 15.10.2020

Inhaltsverzeichnis

A. Auftrag und Auftragsdurchführung....4
B. Zusammenfassung der Ergebnisse....6
C. Analyse des Browsers Protect....6
D. Beurteilung ob Voraussetzungen für eine Softwareprüfung/Zertifizierung im Sinne des IDW PS 880 gegeben sind bzw. als notwendig angesehen werden....8

Anlagen

Anlage 1 Allgemeine Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften

Verzeichnis der Abkürzungen

AGB	=	Allgemeine Geschäftsbedingungen
Abs.	=	Absatz
BAIT	=	Bankaufsichtlichen Anforderungen an die IT
FAIT	=	Fachausschuss für Informationstechnologie
GmbH	=	Gesellschaft mit beschränkter Haftung
MaRisk	=	Mindestanforderungen an das Risikomanagement
PS	=	Prüfungsstandard
Tz.	=	Textziffer
WPG	=	Wirtschaftsprüfungsgesellschaft

A. Auftrag und Auftragsdurchführung

1 Die CORONIC GmbH (im Folgenden: CORONIC) hat uns mit Schreiben vom 20.08.2020 mit einer fachlichen Stellungnahme zur Rechnungslegungs-, Risikomanagement- und Informationssicherheits-Relevanz von Protect (im Folgenden: Stellungnahme) beauftragt.

2 Nach Kontaktaufnahme am 28. Juli 2020 durch Herrn Dr. Frank Bock (Geschäftsführer) und telefonischer Abstimmung zwischen Herrn Dr. Frank Bock Herrn Wirtschaftsprüfer Alexander Beck (AWADO GmbH WPG/StBG) sowie mit entsprechendem Auftragsschreiben wurde die nachfolgende Ausgangssituation dargelegt.

3 Bei der CORONIC GmbH handelt es sich um ein IT-Unternehmen mit Sitz in Kiel, das Finanzdienstleister bei der Entwicklung, Absicherung und Härtung von Bank- und Kaufprozessen im Internet unterstützt.

4 CORONIC hat mit dem Produkt Protect einen gehärteten Browser entwickelt, mittels dem Browser- und Windowsfunktionen sowie alle Seitenaufrufe kontrolliert genutzt werden können. Mit dem Einsatz von Protect soll sichergestellt werden, dass man sich nur auf den sicheren Seiten der Bank und denen der angeschlossenen Verbundpartner bewegen kann.

5 Die vorliegende Stellungnahme erfolgt auf Wunsch der Geschäftsführung und beinhaltet die Beurteilung, ob es sich bei Protect um ein Produkt handelt, das keinen Bezug zur Rechnungslegung oder dem Internen Kontroll- bzw. Risikomanagementsystem im Sinne des §25a KWG bzw. den MaRisk und den BAIT aufweist.

6 Auf Basis der vorgelegten Informationen (vgl. Abschnitt D) sowie der geführten Gespräche beurteilen wir in diesem Zusammenhang, ob für das Produkt Protect der Inhalt einer Softwareprüfung/Zertifizierung im Sinne des IDW PS 880 relevant ist bzw. als notwendig angesehen werden. Im Fokus steht dabei die Analyse des Funktionsumfangs und des Einsatzbereichs für das Produkt Protect.

7 Diese Stellungnahme stellt keine Softwareprüfung oder eine Bescheinigung im Sinne der Informationssicherheit dar. Eine explizite Prüfung und Wertung des Softwareentwicklungsprozesses war nicht Gegenstand dieser Stellungnahme.

8 Neben den MaRisk / BAIT Vorgaben werden bei der fachlichen Stellungnahme auch die Prüfungsstandards PS 880 sowie der IDW RS FAIT 1 berücksichtigt.

9 Das Ergebnis wird im Rahmen der vorliegenden Stellungnahme konsolidiert und dient den Banken zur eigenständigen Einschätzung der Notwendigkeit eines Softwarezertifikats.

10 Als operativer Ansprechpartner des IT-Unternehmens CORONIC wurden am 26. August 2020 Herr Dr. Frank Bock (Geschäftsführer) sowie Frau Lena Schwitalla benannt, insbesondere für entsprechende Auskünfte sowie der Bereitstellung benötigter Unterlagen.

11 Die Stellungnahme ist in die Beschreibung des Auftrags sowie der Auftragsdurchführung (Abschnitt A), der Zusammenfassung der Ergebnisse (Abschnitt B) und in die nachfolgenden Unterpunkte entsprechend der Auftragsabstimmung aufgeteilt:

Abschnitt C – Analyse des Browsers Protect: Auf Basis der vorgelegten Informationen wird das Produkt Protect kurz dargestellt, insbesondere mit dem Fokus der Darstellung des Anwendungsbereichs und möglicher Schnittstellen zur Rechnungslegung, zum Risikomanagement und zur Informationssicherheit des Browsers.

Abschnitt D – Beurteilung ob Voraussetzungen für eine Softwareprüfung/Zertifizierung im Sinne des IDW PS 880 gegeben sind bzw. als notwendig angesehen werden: In diesem Abschnitt erfolgt ein Soll-Ist-Abgleich des Produkts Protect in Bezug ob die allgemein zugänglichen Kriterien für eine Softwareprüfung gemäß IDW PS 880 gegeben sind.

12 Der Auftrag wurde durch Herrn Michael Grabbe durchgeführt. Die Qualitätssicherung erfolgte durch Herrn Wirtschaftsprüfer Alexander Beck.

13 Die nachfolgenden Unterlagen wurden im Zeitraum vom 02. September bis 01. Oktober 2020 durch das IT Unternehmen CORONIC bereitgestellt und stellen die Beurteilungsbasis der nachfolgenden Stellungnahme ab:

- Anwenderhandbuch für die Endkunden
- Entscheidungshilfe NPP
- Ergebnisberichte zu Penetrationstests
- Dokumentation zum Release 5.0
- Exemplarische Log-Datei

14 Die Erstellung dieser Stellungnahme haben wir in unseren Räumen vorgenommen.

15 Die nachfolgende fachliche Stellungnahme bezieht sich ausschließlich auf das Produkt Protect und kann nicht auf andere, ähnliche Browser Produkte übertragen werden.

16 Wir weisen darauf hin, dass die Auskunft aufgrund der heutigen Gesetzeslage gegeben wird, zukünftige Gesetzesänderungen könnten zu einer anderen Beurteilung führen.

17 Die Beurteilung beinhaltet keine weiterführende – über den genannten Auftragsgegenstand hinausgehende – Prüfung des Produkts. Auch eine Bewertung zukünftiger Updates oder sonstiger Veränderungen kann aus den Aussagen der Stellungnahme nicht abgeleitet werden.

18 Die Berichterstattung erfolgt ausschließlich an das IT-Unternehmen CORONIC. Soweit wir Hinweise oder Handlungsempfehlungen geben, haben diese unverbindlichen Charakter. Es obliegt der Geschäftsführung oder sonstigen Empfängern unseres Berichtes, die eigenständige Würdigung der Sachverhalte und eigenverantwortliche Ableitung von Entscheidungen selbst vorzunehmen.

19 Auch soweit wir Empfehlungen oder Hinweise für uns sinnvoll erscheinende Handlungen oder Verhaltensweisen geben, ist jeder Empfänger unserer Berichte oder Darstellungen nicht von seiner Verpflichtung entbunden, sorgfältig und selbständig eine von ihm vorzunehmende unternehmerische Entscheidung vorzubereiten und in eigener Verantwortung zu treffen.

20 Die fachliche Stellungnahme darf vorbehaltlich unserer ausdrücklichen, schriftlichen Zustimmung nur in vollem Wortlaut einschließlich der mit dieser gutachterlichen Stellungnahme fest verbundenen schriftlichen Erklärung über den Zweck des Auftrags, der Weitergabebeschränkung und den Haftungsbedingungen und nur dann an Dritte

weitergegeben werden, wenn sich der jeweilige Dritte zuvor schriftlich mit der Geltung der Allgemeinen Auftragsbedingungen in der Fassung vom 1. Januar 2017 sowie damit einverstanden erklärt hat, den Bericht seinerseits vertraulich zu behandeln und nicht weiterzugeben. Dritte im Sinne dieser Regelung sind nicht verbundene Unternehmen des Instituts, sofern Sie diese vor der Weitergabe umfassend schriftlich über die Bedingungen dieses Auftrags und die zugrundeliegende Haftungsbeschränkung aufklären. Sie werden uns von allen Schadenersatzansprüchen und Kosten freistellen, die sich aus einer Verletzung dieser Weitergabebeschränkung ergeben.

21 Für die Durchführung des Auftrages und unsere Verantwortlichkeit, auch im Verhältnis zu Dritten, gelten die als Anlage zu diesem Schreiben beigefügten „Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften“ in der Fassung vom 1. Januar 2017. Hinsichtlich unserer Haftung verweisen wir auf Ziffer 9 der Allgemeinen Auftragsbedingungen; die Haftung für unsere Tätigkeit ist entsprechend beschränkt.

B. Zusammenfassung der Ergebnisse

22 Bei dem von der CORONIC GmbH entwickelten Produkt Protect handelt es sich um einen gehärteten Internet Browser für Desktopsysteme, der den Bankkunden unter anderem beim Online-Banking über die Homepage der Bank einen erweiterten Schutz vor Angriffen und Schadsoftware bietet.

23 PROTECT bietet funktionell keine Unterschiede zu anderen bekannten Browsern. Abweichungen ergeben sich durch erweiterte Schutzmaßnahmen unter anderem bedingt durch die Kapselung, bei der z.B. beim Start des Browsers automatisiert direkt die Homepage der gewünschten Bank aufgerufen wird.

24 Aufgrund der Einschränkung der Funktionen des Bank-Browsers Protect auf die eigenen Seiten der Bank, und der zusätzlichen getroffenen technischen Schutzverfahren ist, von einem hohen Maß an Sicherheit auszugehen.

25 Da es sich bei Protect lediglich um einen Internet Browser handelt, fließen keine Informationen und Daten über betriebliche Aktivitäten direkt in das Rechnungslegungssystem, und damit in die IT-gestützte Rechnungslegung der Bank ein. Der Einsatz Protect stellt somit keinen rechnungsrelevanten IT-gestützten Geschäftsprozess dar. Vor diesem Hintergrund können die Grundsätze ordnungsmäßiger Buchführung bei IT-gestützter Rechnungslegung vernachlässigt werden.

26 Ein Ausfall von Protect ist für den Endkunden als unkritisch anzusehen, da im Notfall ein Rückgriff auf den Standard Browser jederzeit möglich ist.

C. Analyse des Browsers Protect

27 Die Analyse des Browsers Protect erfolgte durch Sichtung der zur Verfügung gestellten Unterlagen sowie Betrachtung im Live-System einer Bank. Eine Verifizierung und Wertung der Sicherheitsmaßnahmen/Verfahren und deren technische Umsetzung sowie des Softwareentwicklungsprozesses war nicht Gegenstand dieser Analyse.

28 Browser dienen als Zugangspunkt zum Internet und zu zahlreichen Anwendungen. Bei Nutzung eines Web-Browsers werden Daten in der Regel auch aus nicht vertrauenswürdigen Quellen geladen. Diese Daten können schädlichen Code (Viren, Trojaner, Spyware etc.) enthalten und den Arbeitsplatzrechner unbemerkt infizieren, so dass ein sicherer Betrieb nicht mehr möglich ist, was wiederum zum Verlust der Verfügbarkeit, Vertraulichkeit und Integrität von schützenswerten Daten führen kann. Somit stellt eine Nutzung von Web-Browsern erst einmal ein Risiko dar.

29 Um die Angriffsoberfläche, die ein gewöhnlicher Browser aufgrund der Vielzahl seiner Funktionalitäten besitzt, zu minimieren, bietet das IT Unternehmen CORONIC den Banken und deren Kunden den Browser Protect an.

30 Protect ist ein sogenannter gehärteter Browser, der den Bankkunden über den direkten Aufruf der Homepage der Bank einen erweiterten Schutz vor Angriffen und Schadsoftware z.B. beim Online-Banking bieten soll. Auskunftsgemäß ist der Browser durch seine Kapselung vor Angriffen von außen und durch eine digitale Signatur (SHA256) vor Manipulation geschützt. Die technischen Schutzverfahren für das Programm beruhen im Wesentlichen auf sieben Sicherheitsprinzipien, wobei jedes einzelne Sicherheitsprinzip durch mehrere hintereinander gestaffelte technische Methoden abgeschottet ist. Die Bedienung gleicht dem eines normalen Browser. Herstellerunterlagen zu durchgeführten Penetrationstests haben uns zur Einsicht vorgelegen.

31 Jede Bank kann seinen Kunden einen individuellen Browser, der mit unterschiedlichen Funktionen und Daten angereichert und kompiliert wurde, zur Verfügung stellen. Das Programm benötigt keine Administrationsrechte und kann direkt vom Desktop ohne Installation oder einer weiteren Konfiguration gestartet werden. Der Zugriff auf vertrauenswürdige Seiten erfolgt über eine vorab definierte Whitelist. Es handelt sich bei Protect um einen Browser, mit dem der Kunde somit nur vorab freigegebene Bank-Webseiten aufrufen kann. Weitergehende Funktionalitäten werden nicht zur Verfügung gestellt.

32 Bei jedem Start von Protect verbindet sich das Programm obligatorisch mit dem Update-Server, wobei automatisiert auf Programmaktualisierungen hin geprüft wird. Ist ein Update verfügbar, erfolgt eine automatische Aktualisierung auf die jeweils neueste Programmversion. Hierbei wird die vorhandene ausführbare Protect-Programmdatei durch eine neuere Version überschrieben, so dass keinerlei Kundeneingriff notwendig ist. Der gesamte Update-Prozess ist Auskunftsgemäß verschlüsselt und durch Zertifikate gegen Manipulationen gesichert.

33 Die Grundfunktionen des Programms können nicht konfiguriert und damit auch nicht fehlkonfiguriert werden. Der Anwender hat lediglich die Möglichkeit, wohl definierte Darstellungskomponenten individuell einzustellen. Im laufenden Betrieb werden alle Sicherheitsmechanismen dauernd überwacht und kontrolliert und in einem verschlüsselten Log-Protokoll festgehalten. Persönliche Informationen und Webinhalte werden hierin grundsätzlich nicht protokolliert.

34 Aufgrund der Einschränkung der Funktionen des Bank-Browsers Protect auf die eigenen Seiten der Bank, und der zusätzlichen getroffenen technischen Schutzverfahren ist, von einem hohen Maß an Sicherheit auszugehen.

35 Ein Ausfall von Protect ist für den Endkunden als unkritisch anzusehen, da im Notfall ein Rückgriff auf den Standard Browser jederzeit möglich ist.

36 Im Rahmen ihres Softwareentwicklungsverfahrens hat die CORONIC unterschiedliche Bereiche wie die technisch allgemeinen Verfahrensvorgaben für den Entwicklungsprozess (Entwicklerregeln, Tools, Versionsverwaltung etc.), das Anforderungsmanagement im Rahmen der regelmäßigen Releaseplanung (Plan-Vorgaben für Funktion, Oberfläche sowie Erweiterungen und neue Kundenanforderungen), die Ergebnisdokumentation im Rahmen des Releasemanagements (Ist-Ergebnis der jeweiligen Entwicklungsphase, Dokumentation der Abweichungen zum Plan) sowie dem Qualitätsmanagement (Test-, Abnahme- und Deploymentergebnisse) definiert.

D. Beurteilung ob Inhalte einer Softwareprüfung/Zertifizierung im Sinne des IDW PS 880 relevant sind bzw. als notwendig angesehen werden

37 Gegenstand von Softwareprüfungen sind Softwareprodukte unabhängig von deren Implementierung und Produktivsetzung beim Softwareanwender. Softwareprodukte sind gemäß IDW RS FAIT 1, Tz. 12, sowohl selbst erstellte als auch von Dritten bezogene IT-Anwendungen. (siehe IDW PS 880 Tz 4)

38 Abhängig von ihrem Funktionsumfang und Einsatzgebiet können Softwareprodukte in unterschiedlichem Maße für die Rechnungslegung oder Steuerung und Überwachung im Unternehmen relevant sein. IT-Anwendungen mit engerem Bezug zur Rechnungslegung dienen der IT-gestützten Abwicklung rechnungslegungsrelevanter Geschäftsprozesse. Dazu gehören neben Finanzbuchführungsprogrammen insb. ERP-Systeme, die über die Finanzbuchführung hinaus weitere Aufgabengebiete, wie etwa Anlagenbuchführung, Materialwirtschaft, Einkauf, Vertrieb und Personalwirtschaft abdecken. (siehe IDW PS 880 Tz 6)

39 Rechnungslegungsrelevante IT-gestützte Geschäftsprozesse sind dadurch gekennzeichnet, dass Informationen und Daten über betriebliche Aktivitäten (bspw. IT-gestützte Materialwirtschaft) direkt in die IT-gestützte Rechnungslegung Eingang finden, und damit aufzeichnungspflichtige Geschäftsvorfälle abbilden. Insbesondere der Einsatz integrierter Softwarelösungen führt dazu, dass Informationen und Daten über betriebliche Aktivitäten direkt (ohne manuelle Eingaben) in das Rechnungslegungssystem, und damit in die IT-gestützte Rechnungslegung, einfließen. (siehe IDW RS FAIT 1 Tz 14)

40 Der originäre Inhalt bzw. die Intention des IDW PS 880 findet, bedingt durch den (siehe Analyse in Abschnitt C. dieser Stellungnahme) erläuterten Funktionsumfang und dem Einsatzgebiet von Protect, keine Anwendung. Der Browser stellt kein Softwareprodukt im Sinne des IDW PS 880 Tz.6 dar. Das Produkt hat keinen engeren Bezug zur Rechnungslegung bzw. rechnungslegungsrelevanten Geschäftsprozessen. Die Funktion Online-Banking steht dem Bankkunden erst nach entsprechender Legitimation zur Verfügung und ist keine Komponente eines Browsers bzw. von Protect.

41 Ebenfalls handelt es sich bei dem Produkt Protect um kein Finanzbuchführungsprogramm, da hiermit keine Aufgabengebiete, wie etwa Anlagenbuchführung, Materialwirtschaft, Einkauf, Vertrieb und Personalwirtschaft abgedeckt werden.

42 Protect verfügt über keine Schnittstelle zur Rechnungslegung oder weiteren Programmen im Sinne des IDW PS 880 oder IDW RS FAIT 1. Es finden somit keine Informationen und Daten über betriebliche Aktivitäten direkt Eingang in die IT-gestützte Rechnungslegung.

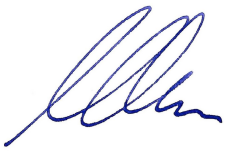
Neu-Isenburg, 15. Oktober 2020

AWADO GmbH

Wirtschaftsprüfungsgesellschaft

Steuerberatungsgesellschaft





Beck
Wirtschaftsprüfer

Grabbe
IT-Prüfer