Entscheidungshilfe für die Einführung des neuen Produktes „gehärteter Protect Browser“

Konzept zur Aufnahme von Aktivitäten bei neuen Produkten oder in neuen Märkten gemäß AT 8.1 MaRisk

CORONIC
Software & Security

0 Verzeichnisse

0.1 Inhaltsverzeichnis

1 Allgemeines zur Entscheidungshilfe

Unsere Anmerkungen reflektieren die nach unserem besten Wissen erfolgte Einschätzung und Interpretation der jeweiligen MaRisk-Abschnitte zum Zeitpunkt der Erstellung dieses Dokuments. Zusätzlich liegt eine Untersuchung der AWADO Wirtschaftsprüfungsgesellschaft zum Protect-Browser vor. Sie stärkt unsere Einschätzung, dass Protect „wie ein ganz normaler Browser" behandelt werden kann, keine wesentliche Auslagerung darstellt und daher ein Neuprodukt-Prozess für die Bank nicht zwingend ist. Betrachten Sie unsere Anmerkungen dennoch als unverbindliche Meinungsäußerungen, ohne dass wir hierfür Haftung übernehmen. Ob und inwieweit Sie sich die folgenden Anmerkungen zu eigen machen und sie in Ihre Prozesse und Überlegungen einbeziehen, obliegt Ihrer eigenen Entscheidung. Sollten Sie die Ausarbeitung eines unter AT 8.1 MaRisk benannten Konzeptes dennoch als notwendig erachten, kann Ihnen dieses Dokument und der Prüfbericht als Hilfestellung dienen.

1.1 Anforderungen gemäß AT 8.1 MaRisk

Bei dem hier vorgestellten Produkt Protect handelt es sich um einen so genannten gehärteten Browser, der den Bankkunden beim Online-Banking über die Homepage der Bank einen erweiterten Schutz vor Angriffen und Schadsoftware bietet. Diese Entscheidungshilfe liefert Ihnen eine Hilfestellung für den Umgang mit den von Ihrem Hause zu beachtenden Vorgaben im Zusammenhang mit neuen Produkten und Märkten gemäß AT 8.1 MaRisk.

Unabhängig von diesen Anmerkungen muss von Ihnen eigenverantwortlich und individuell entschieden werden, ob für die Einführung des Produkts Protect ein Neuprodukt-Prozess notwendig ist oder nicht und falls ja, wie Sie ihn konkret ausgestalten wollen.

1.2 Auszug aus MaRisk und Erläuterungen zum NPP

- Die MaRisk treffen in AT 8.1. u.a. folgende Aussage zum Neuprodukt-Prozess: Jedes Institut muss die von ihm betriebenen Geschäftsaktivitäten verstehen. Für die Aufnahme von Geschäftsaktivitäten in neuen Produkten oder auf neuen Märkten (einschließlich neuer Vertriebswege) ist vorab ein Konzept auszuarbeiten. Grundlage des Konzeptes muss das Ergebnis der Analyse des Risikogehalts dieser neuen Geschäftsaktivitäten sowie deren Auswirkungen auf das Gesamtrisikoprofil sein. In dem Konzept sind die sich daraus ergebenen wesentlichen Konsequenzen für das Management der Risiken darzustellen. (Erläuterung: Inhalt des Konzeptes: Zu den darzustellenden Konsequenzen gehören solche bezüglich der Organisation, des Personals, der notwendigen Anpassung der IT-Systeme, der Methoden zur Beurteilung damit verbundener Risiken sowie rechtliche Konsequenzen (Bilanz- und Steuerrecht etc.), soweit sie von wesentlicher Bedeutung sind).
- Bei der Entscheidung, ob es sich um Geschäftsaktivitäten in neuen Produkten oder auf neuen Märkten handelt, ist ein vom Markt beziehungsweise vom Handel unabhängiger Bereich einzubinden.
- Bei Handelsgeschäften ist vor dem laufenden Handel in neuen Produkten oder auf neuen Märkten grundsätzlich eine Testphase durchzuführen. Während der Testphase dürfen Handelsgeschäfte nur in überschaubarem Umfang durchgeführt werden. Es ist sicherzustellen, dass der laufende Handel erst beginnt, wenn die Testphase erfolgreich abgeschlossen ist und geeignete Risikosteuerungs- und -Controlling Prozesse vorhanden sind.
- Sowohl in die Erstellung des Konzeptes als auch in die Testphase sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten einzuschalten. Im Rahmen ihrer Aufgaben sind auch die Risikocontrolling-Funktion, die Compliance-Funktion und die interne Revision zu beteiligen.

- Das Konzept und die Aufnahme der laufenden Geschäftstätigkeit sind von den zuständigen Geschäftsleitern unter Einbeziehung der für die Überwachung der Geschäfte verantwortlichen Geschäftsleiter zu genehmigen. Diese Genehmigungen können delegiert werden, sofern dafür klare Vorgaben erlassen wurden und die Geschäftsleitung zeitnah über die Entscheidungen informiert wird.
- Soweit nach Einschätzung der in die Arbeitsabläufe eingebundenen Organisationseinheiten Aktivitäten in einem neuen Produkt oder auf einem neuen Markt sachgerecht gehandhabt werden können, ist die Anwendung des AT 8.1 nicht erforderlich

1.3 Einzubindende Organisationseinheiten

Aus bankaufsichtsrechtlichen Gründen sollten bei der Durchführung eines Neuprodukt-Prozess grundsätzlich folgende Bereiche eingebunden werden. Beachten Sie bitte auch unsere konkrete Einschätzung für den Fall von Protect im Abschnitt 6 „Ihre Einschätzung für Protect“

- Interne Revision
- Recht
- Operational Risk Management
- Risikocontrolling
- Rechnungswesen
- Meldewesen
- Notfallmanagement
- Datenschutz
- Compliance & Geldwäsche
- Unternehmenssicherheit
- Zahlungsverkehr

2 Angaben zum Protect und dessen Einführung

2.1 Management Summary

Bei Protect handelt es sich um einen Internet Browser für Desktopsysteme. Er wird vom Endkunden genauso verwendet wie Mozilla Firefox, Google Chrome oder der Microsoft Browser. Allerdings verfügt Protect über erweiterte Schutzmaßnahmen, die das Arbeiten im Online-Banking mit dem Protect Browser sicherer machen, als das Arbeiten mit einem normalen Standard Browser. Vor diesem Hintergrund gestalten sich alle wesentlichen Risiken analog zu den Risiken, die beim Einsatz eines Standardbrowsers erfolgen. Auch der Ausfall von Protect ist für den Endkunden unkritisch, da ein Rückgriff auf den Standard-Browser jederzeit möglich ist. Dieser Gedanke, der Gleichheit in der Nutzbarkeit und Funktion zu allen anderen Standardbrowsern sowie das Ausweichszenario der Nutzung eines Standardbrowsers, halten die Prozesse für Protect schlank und einfach bzw. ermöglichen nach unserer Einschätzung einen Verzicht auf einen Neu-Produkt-Prozess nach AT 8.1 MaRisk für Protect.

2.1.1 Prüfbericht durch die AWADO Wirtschaftsprüfungsgesellschaft

Es liegt ein Prüfbericht der AWADO Wirtschaftsprüfungsgesellschaft zum Protect-Browser vor. Dieser stärkt die Einschätzung, dass Protect „wie ein ganz normaler Browser“ behandelt werden kann. Er ist ein Produkt für Endkunden und wird nicht in der Bank eingesetzt, daher muss der Browser durch die Bank nicht als wesentliche Auslagerung betrachtet werden. Protect verarbeitet laut Bericht keine Zahlungsverkehrs-, Rechnungslegungs- oder Buchhaltungsdaten und kann bei Ausfall durch einen Standard-Browser ersetzt werden. Daher kann dieser durch die Bank als nicht Rechnungslegungs-, Risikomanagement- oder Informationssicherheitsrelevant eingeschätzt werden.

2.2 Zielsetzung und geschäftspolitische Strategie

Das Produkt unterstützt die Strategie der Bank, als verlässlicher und sicherer Partner im Online-Banking aufzutreten. So können heute noch zögernde Kunden von der Nutzung des Online-Banking überzeugt werden und es kann besonders sicherheitsaffinen Nutzern (wie Geschäftskunden) mehr Schutz geboten werden. Die Nutzung von Protect eignet sich als Kundenvorteil und Mehrwert im Kontomodell. Protect ist ein weiterer Baustein im Wettbewerb mit anderen (Direkt-)Banken und Drittdienstleistern (PSD2). Vorteile für die Bank:

- Vermeidung von Schadensfällen im Online-Banking
- Erhöhung der Sicherheit bei allen Online-Finanzgeschäften in der ganzen Gruppe
- Reduzierung der Belegkosten beim Wechsel von Offline-Kunden zu Protect
- Neue Erlösquelle im Online-Banking (als Bezahl-Produkt)
- Kunden-Mehrwert
- Bonuselement im Kontomodell
- Alleinstellungsmerkmal der Bank vor Ort
- Verbesserung des Bank-Image (innovativ, sicherer, modern)
- Stärkt die Kundenbindung (Sicherheit & Vertrauen)
- Überzeugt skeptische Kunden, das Online-Banking zu nutzen

2.3 Produktbeschreibung Protect

Protect ist ein so genannter gehärteter Browser, der den Bankkunden beim Online-Banking über die Homepage der Bank einen erweiterten Schutz vor Angriffen und Schadsoftware bietet. Die Bedienung erfolgt wie bei einem normalen Browser. Allerdings wird mit ihm direkt die Homepage der Bank aufgerufen. Der Browser ist durch seine Kapselung vor Angriffen von außen geschützt. Eine zeitaufwändige Installation oder Konfiguration auf dem Kunden- bzw. Bankkundenrechner ist dabei nicht notwendig. Protect kann einfach z.B. auf dem Desktop des Kundenrechners abgelegt werden und kann von dort per Doppelklick gestartet werden und ist sofort nutzbar. Zur Ausführung sind keine Administratorrechte erforderlich. Beides sorgt für eine deutlich einfachere Nutzbarkeit mit weniger Anforderungen, als dies bei einem normalen Standardbrowser der Fall wäre. Updates werden automatisch beim Start der Anwendung geladen, sodass die verwendete Version immer in der aktuellsten Ausführung genutzt wird. Wird beim Start des Browsers eine Kompromittierung, z.B. durch Schadsoftware, des Kunden-PC festgestellt, wird dies erkannt und gemeldet. Der Protect ist eine Software, die aktuell unter Microsoft Windows und Apple macOS genutzt werden kann.

2.4 Sicherheit von Protect

Protect ist durch eine digitale Signatur (SHA256) vor Manipulation geschützt. Manipulationen an der ausführbaren Datei (z.B. durch Schadsoftware oder vorsätzliche Handlung) können so erkannt werden. Zudem verwendet Protect Techniken wie Certificate Pinning, um die Identität des Webservers auch bei Man-In-The-Middle-Angriffen zweifelsfrei prüfen zu können. Für die Netzwerkkommunikation werden eigene Bibliotheken eingesetzt, so dass auch Angriffe auf die Netzwerkschicht des Betriebssystems verhindert werden können. Die Updateroutine setzt ebenfalls auf digitale Signaturen, um die Authentizität und Integrität der Updates sicherzustellen. Manipulierte Versionen von Protect können so im Rahmen der Updates erkannt werden (nur Updates aus vertrauenswürdiger Quelle werden installiert). Herstellerunterlagen zu durchgeführten Penetrationstests liegen vor.

2.5 Funktionen von Protect

Protect verfügt über die gleichen Funktionen wie ein normaler Standardbrowser. Es gibt daher fachlich keine Unterschiede zur Benutzung von anderen Internet-Browsern. Allein die erhöhte Sicherheit bedingt einige Abweichungen in der Funktion:

- Protect startet automatisch auf der Internetseite der Bank
- Die Sicherheitsfunktionen von Protect verhindern das Wechseln auf unsichere Internetseiten
- Das Update wird aus Sicherheitsgründen vollautomatisch durchgeführt, man kann nicht mit einer veralteten Browserversion arbeiten

2.6 Auswirkungen auf die Endkundenbeziehung

Durch die Einführung des Protect ergeben sich positive Auswirkungen auf die Endkundenbeziehung, da die Bank als sicherheitsbewusster Partner im Online-Banking wahrgenommen wird.

2.7 Definition des Marktes und Marktkompatibilität des Produkts

Protect ist durch seine Funktion als Internet-Browser voll marktkompatibel und erfüllt alle Anforderungen, die vom Online-Banking an einen Internet-Browser gestellt werden. Das Produkt grenzt sich gegenüber anderen Browsersystemen allein durch seine Sicherheitsfunktionen ab und kann daher als sicherste Version für browserbasiertes Online-Banking bezeichnet werden.

2.8 Vertrieb

Protect kann dem Endkunden wie jedes andere normale Programm zur Verfügung gestellt werden:

- Als gepackte Datei (ZIP) im elektronischen Postkorb
- Als Download-Link im gesicherten Bereich des Online-Bankings
- Als Download-Link direkt auf der Homepage der Bank

2.9 Markteinführung

Mögliche Maßnahmen zur Produkt-Einführung sind:

- Homepage pflegen (Downloadlinks eintragen)
- Bankindividuelles Branding klären (Hersteller bietet Vorlagen an)
- Mitarbeiter informieren (Hersteller bietet Textvorlagen an)
- Vertriebsmaterial erstellen (Hersteller bietet Flyer an)
- Produktkatalog pflegen
- Support für Bank klären (Support für die Bank ist im Produktpreis enthalten)
- Endkundensupport klären (Hersteller bietet zusätzlichen Endkundensupport an)
- Ausgabe / Verteilung der Software klären

2.10 Betriebswirtschaftliche Analyse

Der gehärtete Browser Protect wird von der CORONIC GmbH betrieben und supportet. Die Kosten belaufen sich auf:

- monatlicher Grundpreis: 150 €
- zzgl. monatlicher Preis je aktivem Online-Banking-Kunden: 0,015 €

In den Kosten enthalten ist Betrieb, Wartung, stetige Aktualisierung des Produktes sowie 2nd-Level Support für die Bank.

- Einmaliges Setup von 990 € je Bank, enthalten ist …
    - die Erstellung einer bankindividuellen Version von Protect (Text-Branding),
    - die Beratung zum Einsatz des Produktes Protect als Instrument zur Kostenreduzierung und Erlösgenerierung in der Bank,
    - die Unterstützung mit Informationstexten für Mitarbeiter und Endkunden,
    - sowie Werbebanner für die Internetseite der Bank.

Enthalten ist die Bereitstellung, Betrieb, Wartung und stetige Aktualisierung des Produktes sowie 2nd-Level Support für die Bankmitarbeiter.

- Optionaler kostenpflichtiger 1st Level Support für Bank-Endkunden durch CORONIC von Mo.-Fr. zwischen 09:00 und 16:00 Uhr, außer an gesetzlichen Feiertagen: monatlicher Preis je aktivem Online-Banking-Kunden: 0,005 € zzgl. 50 € Grundgebühr.

2.10.1 Kostenvorteile auf Seiten der Bank

- Reduzierung der Schadensfälle und Phishingkosten.
    - Erfahrungsgemäß liegt ein typischer Phishingfall in der Größenordnung von 4.000 € Schadensumme zzgl. 2.000 € Verwaltungskosten (Schadensaufnahme, Schadensdokumentation, Geldwäschebericht, Kommunikation mit den Betroffenen und den Behörden).
    - Bei zwei Phishing Fällen im Jahr liegt die Kostenersparnis bei mind. 12.000 € pro Jahr
    - Es hat noch nie einen Schadensfall beim Einsatz von Protect gegeben.
- Reduzierung der Belegkosten (beim Wechsel von Offline-Kunden zu Protect).
    - Einige Häuser konnten im ersten Jahr der Nutzung 10 % ihrer Offline-Kunden (Beleg-Einreicher und SB-Nutzer) für das Produkt Protect gewinnen.
    - Bei unterstellten Vollkosten einer Belegeinreichung von 2 € und drei Belegen pro Monat ergibt sich Einsparpotenzial von 72 € pro Kunde und Jahr
    - Bei unterstellten 20.000 Beleg- und SB-Kunden und nur 5% Wechselquote ergibt das ein jährliches Einsparvolumen von 72.000 €
- Mögliche Erlöse im Kontomodell bzw. im Einzelverkauf
    - Einige Banken bieten das Produkt als Mehrwert in speziellen Kontomodellen bzw. als Einzelprodukt im direkten Verkauf an. Üblich sind Preise von 1 bis 2 Euro pro Kunde und Monat. Bei einer Bank mit ca. 25.000 aktive Online-Banking-Kunden und etwa 5 % Nutzung des Produktes (sicherheitsaffine Kunden, Geschäftskunden), ergeben sich Erlösmöglichkeiten von 15.000 – 30.000 € pro Jahr.
- Sonstiges
    - Imagegewinn, Neukundengewinn, Wettbewerbsvorteile

3 Vertragliche Regelungen

3.1 Vertragspartner

Vertragspartner sind die CORONIC GmbH und die teilnehmende Bank.

3.2 Weitere rechtliche Rahmenbedingungen

3.2.1 Datenschutz

Ein Datenschutzrisiko liegt nicht vor. Es werden keine personenbezogenen Kundendaten mit Dritten ausgetauscht. Der Zugriff erfolgt immer durch den Kunden selbst über die verschlüsselten Seiten der Bank.

3.2.2 Kartellrecht

Nicht relevant (weil der Kunde jederzeit andere Kanäle nutzen kann).

3.2.3 Aufsichtsrecht

Im Rahmen der Einführung sind insbesondere die folgenden aufsichtsrechtlichen Aspekte zu würdigen:

1) Liegt ggf. eine Auslagerung nach § 25b Kreditwesengesetz („KWG“) sowie AT 9 des Rundschreibens 09/2017 (BA) der Bundesanstalt für Finanzdienstleistungsaufsicht („BaFin“) vom 27. Oktober 2017 – Mindestanforderungen an das Risikomanagement („MaRisk“) einschließlich der Ziffer II. 8 des Rundschreibens 10/2017 (BA) der BaFin vom 3. November - Bankaufsichtliche Anforderungen an die IT („BAIT“) vor?
2) Ist die Durchführung eines NPP nach AT 8.1 MaRisk erforderlich?
3) Wird gegen geldwäscherechtliche Vorschriften, sowie gegen Grundsätze, insbesondere bankübliche Geschäfte, verstoßen? (auf Basis einer rein kursorischen Prüfung).

zu 1) Auslagerung

- Für eine Auslagerung muss die Wesentlichkeit eruiert werden. Für die Frage, ob die Auslagerung wesentlich oder unwesentlich ist, muss nach den MaRisk zunächst die Bank auf Grundlage einer Risikoanalyse eigenverantwortlich festlegen, welche Auslagerungen von Aktivitäten und Prozessen unter Risikogesichtspunkten wesentlich sind (AT 9 Tz. 2 MaRisk).
- Allgemein ist eine Auslagerung wesentlich, wenn hierdurch Aktivitäten und Prozesse von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen betroffen sind sowie die Auslagerung dieser Aktivitäten und Prozesse bankaufsichtsrechtlich relevante Risiken, insbesondere Markt-, Kredit, Ausfall-, Abwicklungs-, Liquiditäts-, Reputationsrisiken sowie operationelle Risiken, begründet. Maßgeblich ist auch, ob sich die Auslagerung auf eine betriebliche Aufgabe bezieht, die für die kontinuierliche und ordnungsgemäße Erbringung und Ausübung von Dienstleistungen für Endkunden und Anlagetätigkeiten wichtig ist (Erläuterungen AT 9 Tz. 1 MaRisk).
- Nach unseren bisherigen Ausführungen und unter Beachtung von Kapitel 4 (Risikobetrachtung) sprechen gute Argumente dafür, dass bei der Nutzung des Protect keine Auslagerung gegeben ist.
- Letztlich muss aber jedes Institut eine solche Risikoeinschätzung selbst vornehmen. Diese Begutachtung kann eine solche Risikoanalyse nicht ersetzen. (Zur Risikoeinschätzung vgl. Ziffer 4.)

zu 2) Neuprodukt-Prozess

- Ob ein Neuprodukt-Prozess erforderlich ist, müssen Institute auf Basis einer individuellen Bewertung selbst entscheiden. Gerne unterstützen wir hierbei natürlich. Rechtsrat können wir jedoch nicht erteilen. Die Aufnahme von Protect in den bankeigenen Produkte-Märkte-Katalog sollte jedenfalls erfolgen. Auch eine Risikoanalyse i.S. einer Risikobewertung ist in jedem Fall erforderlich (vgl. Ziffer 4).
- Ein Neuprodukt-Prozess könnte dann entbehrlich sein, wenn alle beteiligten Organisationseinheiten zu dem Schluss kommen, dass die (neuen) Geschäftsaktivitäten sachgerecht gehandhabt werden können (Nutzung der Öffnungsklausel gemäß AT 8.1 Tz. 7 Ma-Risk).
- Maßgeblich für die Entscheidung ist nicht das neue Produkt oder der Markt selbst, sondern die Bearbeitung durch bzw. im Institut. Somit ist auch ein am Markt etabliertes Produkt als neuartig einzustufen, wenn das Institut dieses erstmalig einsetzt. Weiter sind neue Produkte als Geschäfte einzuordnen, bei denen die Kreditinstitute noch über keine ausreichende Erfahrung zur Durchführung dieser Geschäfte verfügen.
- Durch den Einsatz diverser Browser bei den Bankkunden liegen ausreichende Erfahrungen in einer Bank vor. Durch den Einsatz von Protect entstehen keine neuen Geschäfte, es wird lediglich ein anderer Browser eingesetzt. NPP werden auch nicht bei dem Einsatz weitere marktgängiger Browser eingesetzt.

zu 3) GWG-Konformität

- In diesem Kontext ergibt sich kein besonderer Handlungsbedarf mit Einführung von Protect.

3.2.4 Geldwäsche

Geldwäscherechtliche Probleme ergeben sich durch die Einführung nicht, da der Kunde den Regularien des Online-Bankings unterliegt.

4 Risikobetrachtung

Die Analyse des Risikogehalts der neuen Geschäftsaktivität bildet die Grundlage für das zu erstellende Konzept. Im Folgenden möchten wir Ihnen als Mandant helfen, die möglichen Risiken zu identifizieren und diese besser einschätzen zu können. Eine Garantie auf Vollständigkeit können wir an dieser Stelle nicht geben. Im Folgenden werden die von uns identifizierten Risiken kurz dargestellt und analysiert.

4.1 Strategische Risiken

Mit Protect erweitern die Banken ihre Endkundenbeziehungen und ermöglichen den Kunden Online-Banking in einer sichereren Umgebung. Es besteht nur ein geringes Investitionsrisiko. Strategisch ist es für die Bank von Vorteil Schäden durch Trojaner und Angriffe auf den Kunden-PC zu verhindern sowie die Kundenbindung zu stärken. Dies steigert die Reputation.

4.2 Finanzielle bzw. betriebswirtschaftliche Risiken

Da sich der erforderliche Kostenaufwand in einem begrenzten Rahmen hält, ist das mit der Einführung von Protect verbundene finanzielle Risiko überschaubar. Die Kosten des Protect werden durch den Nutzen aus erspartem Schaden oder erzielbaren Erträgen des Vertriebs üblicherweise übertroffen.

4.3 Kredit/Liquiditätsrisiko

Kein Risiko, da kein Finanzprodukt.

4.4 IT-gestützte Risiken

Kein Risiko. Es handelt sich um eine Datei die lediglich auf den Kunden-PC kopiert wird und von ihm wie jeder andere Browser genutzt wird. Der Browser schützt sich selbst vor der Manipulation durch Dritte mit Hilfe von Prüfsummen.

4.5 Operationelle Risiken

Die operationellen Risiken unterscheiden sich grundsätzlich nicht von denen anderer Abläufe innerhalb der Bank. Die Funktionalität reicht technisch nicht in das Online-Banking hinein (andere Browser unterliegen ebenfalls nicht der Prüfung). Natürlich ist Protect, wie jeder andere Browser, ein Teil der Angriffsoberfläche des Endkunden, welcher den üblichen Online-Banking-Vorgaben und -Kontrollen unterliegt.

4.6 Allgemeines Betrugsrisiko

Durch die Verwendung von Protect entstehen wesentlich geringere Risiken für die Kunden und die Bank. Das allgemeine Betrugsrisiko etwa in Form von Identitäts- oder Datendiebstahl und dadurch unautorisiert ausgelöste Zahlungen entspricht dem allgemeinen, ohnehin bereits vorhandenen Risiko des Onlinebankings. Wenn die Bank sich für eine Verteilung aus dem Postfach oder einen Download nach dem Bank-Login entscheidet, ist der Downloadkanal neben der Verschlüsselung zusätzlich durch Alias und PIN gesichert.

4.7 Datenschutzrisiken

Kein Risiko. Es werden keine Kundendaten mit Dritten ausgetauscht. Der Zugriff erfolgt immer durch den Kunden selbst über verschlüsselte Seiten der Bank.

4.8 Reputationsrisiken

Keine erhöhten Risiken. Das Produkt ist vor dem Hintergrund hoher Sicherheitsstandards entwickelt worden und damit in jedem Fall sicherer als ein normaler Browser. Typische Qualitätsprobleme (z.B. Funktionsstörungen) können sich wie bei jedem anderen Browser negativ auf die Kundenzufriedenheit auswirken. Da der Kunde aber bei einer Funktionsstörung jederzeit mit einem alternativen „normalen" Browser arbeiten könnte, stellen selbst Störungen im Protect keine Verhinderung der Nutzung des Online-Bankings durch den Kunden dar.

4.9 Risiken durch mangelnde Produktkenntnisse

Kein Risiko durch mangelnde Produktkenntnisse im Beratungsgeschäft. Es handelt sich um einen Browser, mit dem der Kunde nur Bank-Webseiten aufrufen kann. Andere Funktionen sind nicht möglich.

4.10 Marktpreisrisiko

Kein Risiko, da kein Finanzprodukt.

5 Organisation

Es ergeben sich durch die Einführung von Protect keine Notwendigkeiten für eine organisatorische Umstrukturierung.

6 Ihre Einschätzung für Protect

6.1 Bank-Entscheidung gegen eine Neu-Produkt-Prozess-Dokumentation

Falls Sie sich entscheiden auf eine Neu-Produkt-Prozess-Dokumentation für Protect zu verzichten, sollten Sie dies damit begründen, dass keine Auslagerung und in der Folge auch keine Neu-Produkt-Prozess-Pflicht vorliegt. Diese Entscheidung wird auch vom Prüfbericht der AWADO Wirtschaftsprüfungsgesellschaft gedeckt. Wenn Sie sich dem anschließen, finden Sie im *Abschnitt 2 „Aufsichtsrecht"* unter den Punkten: „*zu 1) Auslagerung*" und „*zu 2)* Neu-Produkt-Prozess", sowie im Prüfbericht, die entsprechende Argumente.

Sie sollten Protect dennoch in den bankeigenen Produkte-Märkte-Katalog aufnehmen.

6.2 Bank-Entscheidung für eine Neu-Produkt-Prozess-Dokumentation

Falls Sie sich dennoch dafür entschieden haben, einen Neu-Produkt-Prozess für die Einführung von Protect durchzuführen, nutzen sie gerne diese Entscheidungshilfe für ihre Dokumentation.

6.2.1 Bank ist Neukunde von Protect

Da das Produkt im Kern wie ein normaler Browser arbeitet, könnten Sie sich für eine Kurzbeschreibung entscheiden:

Produkt- und Funktions-beschreibung	Protect ist ein gehärteter Browser, der unseren Kunden beim Online-Banking über unsere Homepage einen erweiterten Schutz vor Angriffen und Schadsoftware bietet. Die Bedienung erfolgt wie bei einem „normalen" Browser. Allerdings wird von Protect unsere Homepage aufgerufen. Der Browser ist durch seine Kapselung vor Angriffen von außen geschützt. Eine zeitaufwändige Installation oder Konfiguration auf dem Kunden- bzw. Bankkundenrechner ist dabei nicht notwendig. Es genügt, die Browser-Datei auf den Desktop zu kopieren, sie startet mit Doppelklick, ohne Installation und ohne Administratorrechte. Updates werden automatisch beim Start der Anwendung geladen, so dass die verwendete Version immer in der aktuellsten Ausführung genutzt wird. Wird beim Start von Protect eine Kompromittierung, z.B. durch Schadsoftware, des Kunden-PC festgestellt, wird dieser Schädling aus dem Browser-Prozess ausgesperrt, um sichereres Online-Banking zu ermöglichen. In besonders schweren Fällen wird das Banking unterbunden und der Kunde bekommt einen Hinweis mit einer Servicenummer.

	Protect ist eine Software, die aktuell unter Microsoft Windows und Apple macOS genutzt werden kann. ***Vertrieb*** Protect kann dem Endkunden wie jedes andere normale Programm zur Verfügung gestellt werden: • Als gepackte Datei (ZIP) im Postkorb • Als Download-Link im gesicherten Bereich der Online-Geschäftsstelle • Als Download-Link direkt auf der Homepage der Bank ***Sicherheit*** Protect ist durch eine digitale Signatur (SHA256) vor Manipulation geschützt. Manipulationen an der ausführbaren Datei (z.B. durch Schadsoftware oder vorsätzliche Handlung) können so erkannt werden. Zudem verwendet Protect Techniken wie Certificate Pinning, um die Identität des Webservers auch bei Man-In-The-Middle-Angriffen zweifelsfrei prüfen zu können. Für die Netzwerkkommunikation werden eigene Bibliotheken eingesetzt, so dass auch Angriffe auf die Netzwerkschicht des Betriebssystems verhindert werden können. Die Updateroutine setzt ebenfalls auf digitale Signaturen, um die Authentizität und Integrität der Updates sicherzustellen. Manipulierte Versionen von Protect können so im Rahmen der Updates erkannt werden (nur Updates aus vertrauenswürdiger Quelle werden installiert). Herstellerunterlagen zu durchgeführten Penetrationstests liegen vor.
Geschäftspolitische Strategie und Ziele	Das Produkt unterstützt unsere Strategie, als verlässlicher und sicherer Partner im Online-Banking aufzutreten. So können durchaus auch heute noch zögernde Kunden von der Nutzung des Online-Banking überzeugt werden. Protect ist daher ein weiterer Baustein im Wettbewerb mit anderen (Direkt-)Banken und Drittdienstleistern (PSD2). Vorteile für die Bank: • Vermeidung von Schadensfällen im Online-Banking • Erhöhung der Sicherheit bei allen Online-Finanzgeschäften in der ganzen Gruppe • Reduzierung der Belegkosten beim Wechsel von Offline-Kunden zu Protect • Neue Erlösquelle im Online-Banking (als Bezahl-Produkt) • Kunden-Mehrwert • Bonuselement im Kontomodell • Alleinstellungsmerkmal der Bank vor Ort • Verbesserung des Bank-Image (innovativ, sicherer, modern) • Stärkt die Kundenbindung (Sicherheit & Vertrauen) • Überzeugt skeptische Kunden, das Online-Banking zu nutzen

Betriebswirtschaftliche Analyse	Der gehärtete Browser Protect wird von der CORONIC GmbH betrieben und supportet. Die Kosten belaufen sich auf:
	• monatlicher Grundpreis: 150 €
	• zzgl. monatlicher Preis je aktivem Online-Banking-Kunden: 0,015 €
	In den Kosten enthalten ist Betrieb, Wartung, stetige Aktualisierung des Produktes sowie 2nd-Level Support für die Bank.
	• Einmaliges Setup von 990 € je Bank, enthalten ist …
	  ○ die Erstellung einer bankindividuellen Version von Protect (Text-Branding),
	  ○ Unterstützung mit Informationstexten für Mitarbeiter und Endkunden,
	  ○ Vorlagen und Bilder für die Internetseite der Bank.
	Kostenvorteile für die Bank
	• Reduzierung der Schadensfälle beim Phishing (kalkuliert nach typischen Fallzahlen, ggf. bitte die Werte in eckigen Klammern mit den Hauszahlen ersetzen).

	○ Erfahrungsgemäß liegt ein typischer Phishingfall in der Größenordnung von [4.000 €] Schadensumme, zzgl. [2.000 €] Verwaltungskosten (Schadensaufnahme, Schadensdokumentation, Geldwäschebericht, Kommunikation mit den Betroffenen und den Behörden). ○ Bei zwei Phishing Fällen im Jahr liegt die Kostenersparnis bei [12.000 €] pro Jahr ○ Hinweis: die internen Verwaltungskosten fallen auch dann an, wenn das Geld letztendlich nicht entwendet wurde. Auch hier reduziert ein gehärteter Browser die Verwaltungskosten, ohne dass tatsächlich Geld gestohlen wurde. ○ Es hat noch nie ein Schadensfall beim Einsatz von Protect gegeben. • Reduzierung der Belegkosten (beim Wechsel von Offline-Kunden zu Protect). ○ Einige Banken konnten im ersten Jahr der Nutzung 10 % ihrer Offline-Kunden (Beleg-Einreicher und SB-Nutzer) für das Produkt Protect gewinnen. ○ Bei unterstellten Vollkosten einer Belegeinreichung von [2 €] und [drei] Belegen pro Monat ergibt sich Einsparpotenzial von [72 €] pro Kunde und Jahr ○ Bei unterstellten [20.000] Beleg- und SB-Kunden und nur [5%] Wechselquote ergibt das ein jährliches Einsparvolumen von [72.000 €] • Erlöse im Kontomodell bzw. im Einzelverkauf (kalkuliert nach typischen Fallzahlen, ggf. bitte die Werte in eckigen Klammern mit den Hauszahlen ersetzen). ○ Viele Banken bieten das Produkt als Mehrwert in speziellen Kontomodellen bzw. als Einzelprodukt im direkten Verkauf an. Üblich sind Preise von [1 bis 2 Euro] pro Kunde und Monat. Bei unserem Institut mit ca. [25.000] aktiven Online-Banking Kunden und einer minimalen erwarteten Nutzung des Produktes von [5 %] (sicherheitsaffine Kunden, Geschäftskunden), ergeben sich Erlösmöglichkeiten von bis zu [12 Monate x 2 € x 1.250 Nutzer = 30.000 €] pro Jahr. ○ Der Hersteller bietet Beratung bei der Einführung von neuen Kontomodellen unter Zuhilfenahme von Protect an und vermittelt Kontakte zu Banken, die ein solches Modell bereits erfolgreich umgesetzt haben • Sonstiges ○ Imagegewinn, Neukundengewinn, Wettbewerbsvorteile
Risikobetrachtung	***Kredit/Liquiditätsrisiko*** Kein Risiko, da kein Finanzprodukt. ***IT-gestützte Risiken*** Kein Risiko. Es handelt sich um eine Datei die lediglich auf den Kunden PC kopiert wird und von diesem wie jeder andere Browser genutzt wird. ***Operationelle Risiken*** Die operationellen Risiken unterscheiden sich grundsätzlich nicht von denen anderer Abläufe innerhalb der Bank. Die Funktionalität reicht technisch nicht in das Online-Banking hinein (andere Browser unterliegen ebenfalls nicht der Prüfung). Natürlich ist Protect, wie jeder andere Browser, ein Teil der Angriffsoberfläche des Endkunden, welcher den üblichen Online-Banking-Vorgaben und -Kontrollen unterliegt. ***Allgemeines Betrugsrisiko*** Durch die Verwendung von Protect entstehen wesentlich geringere Risiken für die Kunden und die Bank. Das allgemeine Betrugsrisiko etwa in Form von Identitäts- oder Datendiebstahl und dadurch unautorisiert ausgelöste Zahlungen entspricht dem allgemeinen, ohnehin bereits vorhandenen Risiko des Onlinebankings. ***Datenschutzrisiken***

	Kein Risiko. Es werden keine Kundendaten mit Dritten ausgetauscht. Der Zugriff erfolgt immer durch den Kunden selbst über verschlüsselte Seiten der Bank. ***Reputationsrisiken*** Keine erhöhten Risiken. Das Produkt ist vor dem Hintergrund hoher Sicherheitsstandards entwickelt worden und damit in jedem Fall sicherer als ein normaler Browser. Typische Qualitätsprobleme (z.B. Funktionsstörungen) können sich wie bei jedem anderen Browser negativ auf die Kundenzufriedenheit auswirken. Da der Kunde aber bei einer Funktionsstörung jederzeit mit einem alternativen „normalen" Browser arbeiten könnte, stellen selbst Störungen im Protect keine Verhinderung der Nutzung des Online-Bankings durch den Kunden dar. ***Risiken durch mangelnde Produktkenntnisse*** Kein Risiko durch mangelnde Produktkenntnisse im Beratungsgeschäft. Es handelt sich um einen Browser, mit dem der Kunde nur Bank-Webseiten aufrufen kann. Andere Funktionen sind nicht möglich. ***Marktpreisrisiko*** Kein Risiko, da kein Finanzprodukt.
Betriebswirtschaftliche Risiken	Die Kosten für Protect sind mit [500 € pro Monat] überschaubar und sinnvoll (bitte konkrete Zahlen aus dem Angebot in die eckigen Klammern eintragen)
Vertragliche Regelungen	Es wurde ein Nutzungsvertrag geschlossen. Vertragspartner sind die CORONIC GmbH und die teilnehmende Bank.
Notwendige Maßnahmen zur Einführung	Notwendige Maßnahmen zur Produkt-Einführung sind: • Mitarbeiter informieren (Hersteller bietet Textvorlagen an) • Vertriebsmaterial erstellen (Hersteller bietet Vorlagen an) • Produktkatalog pflegen • Homepage pflegen (Hersteller bietet Vorlagen an) • Support für Bank klären (Support für die Bank ist im Produktpreis enthalten) • Verteilung der Software klären (automatische Verteilung über Computercheck) • Bankindividuelles Branding klären (Hersteller bietet Vorlagen an)
Testphase und Fazit	Der Protect wurde durch [Abt. XXX; Mitarbeiter XXX] im Zeitraum [XXX] ausgiebig im Live-Betrieb getestet (bitte konkrete Ansprechpartner aus dem Hause in den eckigen Klammern benennen). Eine darüber hinaus gehende Testphase halten wir für nicht erforderlich. Wir sind zu dem Schluss gekommen, dass die neuen Geschäftsaktivitäten mit Protect sachgerecht gehandhabt werden können.