

# Fragen und Antworten zum S-Protect Browser



Stand 03/2022

## Stimmen zu Protect

Protect ist ein gehärteter Browser. Man kann sich Protect als eine Art Rundumschutz für alle Finanzgeschäfte in der Sparkassen-Finanzgruppe vorstellen. Protect kontrolliert Browser- und Windowsfunktionen sowie alle Seitenaufrufe und sorgt so dafür, dass man sich nur auf den guten, sicheren Seiten der Sparkasse und der angeschlossenen Partnerunternehmen bewegen kann.

*„An die Sicherheit im Online-Banking stellt die Sparkasse Göttingen seit jeher höchste Anforderungen. Denn nur wenn ein Kunde sich sicher fühlt, nimmt er auch aktiv am Online-Banking teil. Dieser einfachen Erkenntnis folgend hat die Sparkasse Göttingen sich für den Einsatz des gehärteten Browsers "Ihr Browser. Sicher." der Firma CORONIC entschieden. Das Produkt ist fester Bestandteil unserer Kontomodelle und schützt jeden Kunden bei jeder einzelnen Überweisung im Netz. Wir können dieses Produkt nur allen anderen Finanzinstituten empfehlen.“*

Matthias Rebhan, stellv. Abteilungsleiter Mediale Zahlungsdienste, Sparkasse Göttingen

*„Der Internet-Browser ist nach wie vor der meistgenutzte Zugangskanal zum Online-Banking. Gleichzeitig ist dieser Kanal auch am anfälligsten für Phishing- und Trojanerangriffe. Sicherheitslücken in gängigen Browsern wie Firefox, Chrome, Edge oder Safari führen dazu, dass Betrüger die Anzeige im Browser manipulieren können, Zugangsdaten stehlen oder betrügerische Überweisungen ausführen können. An dieser Stelle können sogenannte „gehärtete Browser“ die Sicherheit deutlich erhöhen.“*

Auszug aus dem DSGVO Rundschreiben zu, S-Protect Browser

Erklär-Video des Herstellers:

[www.coronic.de/Protect#sProtect](http://www.coronic.de/Protect#sProtect)

## **Liste der allgemeinen Fragen**

- Was ist Protect?
- Was ist das Neue am neuen Protect?
- Wie kann ich Protect an meine Kunden verteilen?
- Warum ist Protect sicherer als ein normaler Browser?
- Warum ist ein normaler Browser nicht sicher?
- Kann man Protect auf einem verseuchten Computer einsetzen?
- Unterstützt Protect die Nutzung des Kontoauswahlmoduls von externen Partnern?
- Wer übernimmt die Hotline bei Problemen mit dem Browser?
- Wie funktioniert der 2nd Level Support?
- Wie funktioniert der 1st Level Support?
- Was ist mein erster Schritt zur Einführung von Protect?
- Wie nutzen andere Banken Protect?
- Welche Betriebssysteme unterstützt Protect?
- Muss Protect installiert werden?
- Prüft der Protect Browser die erforderlichen Systemvoraussetzungen?
- Kann die Startseite der Bank individuell gestaltet werden?
- Wie funktionieren Updates bei Protect?
- Kann ich erkennen, welcher Kunde mit Protect Online-Banking gemacht hat?
- Warum ist Protect „so teuer“?
- Wie aktualisiert sich der Browser und wie ist das Update gegen Phishing geschützt?
- Welche Kontaktdaten sieht der Endkunde im Browser?
- Gibt es Protect auch für mobile Endgeräte?
- Bei Phishing Mails kann Protect aber nichts machen, oder?
- Kann Protect „als Standardbrowser“ die Links in Phishing-Mails abfangen?
- Kann Protect auf beliebig vielen Endgeräten genutzt werden?
- Wie wird Protect wieder deinstalliert?
- Wird eine Schulung oder ein Handbuch für die Nutzung von Protect benötigt?

## **Liste der Fragen zur Nutzung in der S-Finanzgruppe**

- Unterstützt Protect die neuen web-Portale der FI
- Kann man den Browser für den Endkunden verpflichtend machen?
- Wird die Arbeit über SEVA in der FI-Umgebung unterstützt?
- Was bewirkt die Verknüpfung "Gehärteter Browser" im OB-Teilnehmervertrag?
- Muss der Content für die IF selber eingebaut werden oder gibt es zentralen Content?
- Funktioniert der Browser auch mit dem Firmenkundenportal?
- Werden fremde Content-Inhalte in der IF vom Browser ignoriert?
- Gibt es Probleme, wenn Sparkassen Cobra-Inhalte in der IF einsetzen?
- Woher bekommen Sie die Zahl der aktiven Online-Banking Kunden
- Gibt es bei Druck der Erstzugangsdaten Informationen über S-Protect dazu?

### **Was ist Protect?**

Protect ist ein so genannter gehärteter Browser. Er verhindert, dass Trojaner und andere Schadprogramme in das Online-Banking eingreifen und Geld klauen. Das Programm besteht aus einer circa 10 MB großen EXE-Datei. Diese Datei kann einfach auf den Desktop gelegt werden und ist sofort per Doppelklick lauffähig. Protect muss nicht installiert werden, benötigt keinerlei Konfiguration und keine Administratorrechte. Protect kann auch auf einem bereits durch Viren und Trojaner verseuchten PC eingesetzt werden und sorgt dort trotzdem für sichereres Online-Banking. Innerhalb von Protect können keine manipulierten Internetseiten geladen werden. Eine Umlenkung auf Phishing-Sites wird verhindert. Im Protect-Browser können Sicherheitsmerkmale und Kontoinformationen nicht ausgelesen werden.

### **Was ist das Neue am neuen Protect?**

Protect war bisher ein reiner Online-Banking-Browser. Wer sicher Geld überweisen wollte nahm Protect. Wenn man sich sonst auf den Seiten der Bank oder den Internetseiten der Partnerunternehmen bewegen wollte, musste man einen konventionellen Browser nutzen. Seit 2021 ist eine neue Produktversion verfügbar, mit der man sich frei auf allen Seiten der gesamten Finanzgruppe bewegen kann. Heute lassen sich alle Kundenreisen komplett in Protect darstellen, auch wenn diese bei der Bausparkasse oder der Versicherung enden. Diese neue Freiheit bezieht auch Dienstleister der Finanzgruppe mit ein. So haben viele Banken ihr Sortengeschäft mit ausländischen Währungen an die Reisebank ausgegliedert, nutzen den Kontomodellfinder eines externen Partners oder binden Servicemodule anderer Finanzdienstleister in ihre eigene Internetseite ein. Der neue Protect spannt seinen Sicherheitschirm über all diese Internetseiten und erlaubt so sicherere Finanzgeschäfte in der gesamten Finanzgruppe.

### **Wie kann ich Protect an meine Kunden verteilen?**

Die Verteilung kann per Download oder über ein Speichermedium erfolgen, z. B.

- > Aus einem passwortgeschützten Kunden- oder Mitgliederbereich
- > Direkt aus dem Online-Banking-Postkorb
- > Download im Online-Banking aus dem Aktionskanal rechts auf der Seite
- > Offener Download von der Homepage der Bank
- > Verteilung vom USB-Speicherplatz im Kartenlesegerät

### **Warum ist Protect sicherer als ein normaler Browser?**

Viele Trojaner greifen nicht mehr das Banking-Verfahren, sondern den Banking-Nutzer an. Durch gefälschte Einblendungen im Browser (z.B. Rücküberweisungs-Trojaner) und Social-Engineering wird der Nutzer manipuliert. Wird der Zugriff der Trojaner auf den Internetbrowser verhindert, können alle dahinter ablaufenden Online-Geschäftsprozesse nicht mehr manipuliert werden. Protect übernimmt genau diesen Schutz des Internetbrowsers. Protect

kontrolliert Browser-, Netzwerk- und Windowsfunktionen sowie alle Seitenaufrufe und sorgt so dafür, dass man sich nur auf den sicheren Seiten der Bank bewegen kann. Die Sicherheit ist auch bei neuen Trojaner-Generationen gegeben, da alle Schädlingfunktionen im Browser durch geprüfte Anti-Hooking- und Anti-Cracking-Mechanismen unterdrückt werden.

### **Warum ist ein normaler Browser nicht sicher?**

Die Aufgabe eines Browsers ist es, jede Internetseite anzuzeigen und jedes Video abzuspielen. Damit ist ein Browser das genaue Gegenteil einer sicheren Software, denn er erlaubt alles. Die Angriffsmethoden von Viren- und Trojaner-Herstellern basieren daher technisch immer auf der Manipulation von Browserfunktionen. So werden HTML-Seiten im Browser verändert und der Nutzer mit gefälschten Einblendungen getäuscht. Moderne Banking-Trojaner haben sich daher schon vor Jahren auf die Manipulation der Banking-Seiten im Browser spezialisiert. Mit gefälschten Überweisungen, vermeintlichen Gerätetests oder vorgetäuschten Retourenaufträge klauen diese Schädlinge das Geld des unbedarften Kunden, indem sie die Darstellung im Browser manipulieren. Eine moderne Sicherheitskonzeption muss daher direkt beim Browser ansetzen. Wird der Zugriff von Trojaner auf den Internetbrowser verhindert, können alle dahinter ablaufenden Online-Geschäftsprozesse (z.B. Banking) nicht mehr manipuliert werden.

### **Kann man Protect auf einem verseuchten Computer einsetzen?**

Protect kann auch auf einem bereits durch Viren und Trojaner verseuchten PC eingesetzt werden und sorgt trotzdem für sichereres Online-Banking als ein normaler Browser. Bei Kenntnis über einen verseuchten PC sollte darauf aber kein Online-Banking mehr gemacht, sondern Viren und Trojaner entfernt werden.

### **Unterstützt Protect die Nutzung des Kontoauswahlmoduls von externen Partnern?**

Ja. Ganz grundsätzlich gilt: alle Seiten und Funktionen, die benötigt werden, um sich innerhalb der S-Finanzgruppe zu bewegen und Produkte abzuschließen, werden unterstützt. Das bedeutet alle Kundenreisen können im Protect Browser zu Ende geführt werden, ganz egal ob sie bei der Deka, der Provinzial oder auf Seiten des Kontoauswahlmoduls einer Beratungsfirma enden.

### **Wer übernimmt die Hotline bei Problemen mit dem Browser?**

CORONIC übernimmt den Support für die Bank. Der Endkunde meldet sich zunächst bei der Bank. Wenn es sich um ein technisches Problem handelt, leitet die Bank den Call an CORONIC weiter. Es besteht die Möglichkeit bei Vertragsabschluss auch den Endkunden Support komplett an CORONIC auszugliedern. Erfahrungsgemäß gibt es nach Einführung des Produktes ein oder zwei Monate einige Anrufe in der Hotline, danach hält sich der Endkunden-Support jedoch in engen Grenzen, denn das Produkt ist „ja nur ein Browser“ und jeder

weiß, wie man mit einem Browser umgeht. CORONIC liefert sowohl für die Endkunden als auch für die Bankmitarbeiter ein eigenes Supporthandbuch mit aus.

### **Wie funktioniert der 2nd Level Support?**

Im Produktpreis enthalten ist der 2nd Level Support für die Mitarbeiter der Bank. Die Bank kann über die E-Mail-Adresse [sProtect@coronic.de](mailto:sProtect@coronic.de) Supportanfragen in das Ticketsystem von CORONIC geben. Daneben steht zu den normalen Arbeitszeiten eine Telefonnummer für den Support der Bankmitarbeiter zur Verfügung: 0431 530 273-31. Servicezeiten sind montags bis freitags zwischen 09:00 und 16:00 Uhr, außer an gesetzlichen Feiertagen.

### **Wie funktioniert der 1st Level Support?**

Der Support für die Endkunden der Bank ist nicht im Standard Produktpreis enthalten. 1st Level Support kann jedoch als kostenpflichtige Option dazugekauft werden. Falls Sie diese Option gewählt haben, stellt CORONIC eine zentrale E-Mail-Adresse für ihre Endkunden zur Verfügung. Anfragen an diese Adresse werden im COR-Ticketsystem erfasst. Der COR-Support tritt dann in direkten Kontakt mit Ihren Endkunden, um deren Fragen zum Produkt zu klären. Servicezeiten sind montags bis freitags zwischen 09:00 und 16:00 Uhr, außer an gesetzlichen Feiertagen.

### **Was ist mein erster Schritt zur Einführung von Protect?**

Tip 1 - Erstmal einen SB-Automaten abschalten: Im Controlling erfragen, wo kaum genutzte (d.h. von weniger als 200-400 Kunden) SB-Überweisungsautomaten stehen. Die wenigen Kunden einzeln ansprechen und Protect erklären. Ein Automat erzeugt jährliche Kosten im vierstelligen Eurobereich, die mit dieser einmaligen Aktion entfallen.

Tip 2 - Erstmal die Belegkosten einer Filiale reduzieren: Unter den Belegkunden einer Filiale sind erfahrungsgemäß die meisten Kunden „Offliner wider Willen“. D.h. sie nutzen Smartphone und PC im Internet, verweigern aber aus Angst beklaut zu werden das Online-Banking. Belegkunden selektiv ansprechen und Protect erklären.

Tip 3 - Breite Verteilung an alle Kunden: Bewerben Sie Protect mit Hilfe unserer Werbebilder am Geldautomaten, SB-Überweisungsautomaten oder digitalen Schaufenster und bieten Sie Protect allen Kunden bequem als Download auf der Webseite an

Tip 4 – Firmenkunden ansprechen: Bei Firmenkunden, die keine Software, sondern einen normalen Browser für ihr Banking nutzen, Protect verteilen.

### **Wie nutzen andere Banken Protect?**

Das Protect Phishing und damit auch die Folgekosten von Online-Trojanern erfolgreich verhindert, ist allgemein bekannt. Neben diesem naheliegenden Anwendungsgebiet gibt es jedoch eine Reihe von anderen Einsatzszenarien. Sie reichen von neuen Erlösmodellen, Neukundenakquise und Marketing bis zu Kosteneinsparungen im Belegbanking. Wenn Sie eine

individuelle Einführungsstrategie für Protect planen, fragen Sie uns gerne, wir helfen mit konkreten Beispielen und Excel-Kalkulationen für die Vorstandsvorlage weiter. Hier einige typische Beispiele von Banken, die Protect erfolgreich und gewinnbringend einsetzen.

Protect als Kostenbremse: Viele Banken schaffen es mit Protect auch eingefleischte Offliner zu begeisterten Online-Kunden zu machen. Wesentlich ist hierbei das Sicherheitsversprechen gegenüber dem Kunden, denn nur wer sich wirklich sicher fühlt, nimmt auch aktiv an Online-Geschäftsprozessen teil.

Belegkosten reduzieren: Die meisten Belegkunden würden gerne Online-Banking machen, lehnen es jedoch aus Sicherheitsbedenken ab. Mit Protect haben es einige Häuser geschafft, ihre Belegkundenzahl binnen Jahresfrist um mehr als 10% zu reduzieren. Bei typischen Belegkosten in Vollkostenrechnung von 25-50 € pro Jahr kann so leicht ein sechsstelliger Eurobetrag pro Jahr eingespart werden.

SB-Überweisungsautomaten abschalten: Bei vielen Banken werden die SB-Überweisungsautomaten nur von wenigen hundert Kunden genutzt. Einzelne Geräte weisen sogar nur zweistellige Nutzungszahlen auf. Wechseln diese Kunden ins sicherere Online-Banking mit Protect, können diverse SB-Automaten mit Jahreskosten im vierstelligen Bereich dauerhaft abgeschaltet werden.

Protect als neues Erlösmodell: Viele Banken setzen Protect als zusätzliche Sicherheitsoption im Rahmen eines neuen Kontomodells ein. Zum Online-Konto gehört dann automatisch auch Protect und mit ihm das Versprechen, für sicheres Online-Banking zu sorgen. Einige Kunden haben mit diesem Ansatz im ersten Betriebsjahr ihre Online-Quote um mehr als 10% erhöht, d.h. 10% aller Kunden zahlen jetzt einen monatlichen Zuschlag zur Kontogebühr.

Protect als Online-Mehrwert: In der Nacht sind alle Katzen grau und so gleicht auch ein Online-Banking meist dem anderen. Um sich im Wettbewerb zu differenzieren und dem Kunden einen echten Online-Mehrwert anzubieten ist Protect der richtige Kandidat.

### **Welche Betriebssysteme unterstützt Protect?**

Protect ist lauffähig unter allen aktuell vom Hersteller unterstützten Windows und MacOS Betriebssystemen.

### **Muss Protect installiert werden?**

Nein. Das Programm besteht aus einer einzigen EXE-Datei. Diese Datei kann einfach auf den Desktop kopiert werden und ist sofort per Doppelklick lauffähig. Protect muss nicht installiert werden, benötigt keinerlei Konfiguration und keine Administratorrechte.

### **Prüft der Protect Browser die erforderlichen Systemvoraussetzungen?**

Protect unterstützt standardmäßig alle Betriebssysteme, für die der Hersteller noch Sicherheitsupdates herausgibt. Eine explizite Prüfung findet jedoch nicht statt. Wir finden den Vorschlag aber gut und werden diese Überprüfung in der nächsten Version implementieren.

### **Kann die Startseite der Bank individuell gestaltet werden?**

Es wird eine URL als Landingpage hinterlegt. Diese kann die Bank frei auswählen oder aber standardmäßig auf der Homepage oder der Online-Banking Seite starten.

### **Wie funktionieren Updates bei Protect?**

Bei jedem Start von Protect wird Online zunächst die Aktualität der verwendeten Programmversion kontrolliert. Ist ein Update verfügbar, erfolgt eine automatische Aktualisierung auf die jeweils neueste Programmversion. Dabei wird die vorhandene Protect EXE-Datei durch eine neuere Version überschrieben, so dass keinerlei Kundeneingriff notwendig ist. Der gesamte Update-Prozess ist verschlüsselt und durch Zertifikate gegen Manipulationen gesichert.

### **Kann ich erkennen, welcher Kunde mit Protect Online-Banking gemacht hat?**

Ja. Protect verwendet einen eigenen Browsernamen (ähnlich dem „browser agent“), den man in der bankinternen Statistik wiederfinden kann. So besteht jederzeit die Möglichkeit einer Zuordnung, ob eine Überweisung mit dem gehärteten Browser erfolgt ist oder nicht.

### **Warum ist Protect „so teuer“?**

Protect ist eine komplexe, mehrschichtige Sicherheitssoftware. Protect sorgt dort für Sicherheit, wo Betriebssystem und Netzwerkschicht auf dem PC versagen. Protect muss sozusagen die Lücken stopfen, die Microsoft, Apple und andere Hersteller offengelassen haben, denn diese Lücken sind in der Vergangenheit stets Zugangstüren für Banking-Trojaner gewesen. Das bedeutet aber auch, dass sich mit jeder Veränderung am Computer (z.B. Windows Update) auch Protect ändern und den neuen Gegebenheiten anpassen muss. Dieses dauernde Überarbeiten und Testen der Sicherheitsmechanismen ist sehr personalaufwändig und teuer.

### **Wie aktualisiert sich der Browser und wie ist das Update gegen Phishing geschützt?**

Die Aktualisierung erfolgt über einen Update-Server. Update-Server und Protect-Client erkennen sich gegenseitig anhand ihrer Zertifikate. So wird verhindert, dass ein Update von einem anderen Server stattfinden kann. Protect prüft bei jedem Programmstart die Softwareversion und installiert gegebenenfalls automatisch die neueste Version.



### **Welche Kontaktdaten sieht der Endkunde im Browser?**

Welche Kontaktdaten angezeigt werden, kann jede Bank selbst entscheiden. Auch das Design, der Splashscreen beim Start, der Name und im gewissen Umfang die verwendeten Texte im Browser sind individualisierbar.

### **Gibt es Protect auch für mobile Endgeräte?**

Derzeit nicht, sollten sich genügend Banken interessieren, würden wir das einplanen.

### **Bei Phishing Mails kann Protect aber nichts machen, oder?**

Bei den „Microsoft-Anrufen“, bei denen die Kunden am Telefon dazu verleitet werden „freiwillig“ Geld zu überweisen, hilft natürlich weder Protect, noch irgendeine andere Sicherheitssoftware, denn der Kunde denkt ja, er macht es wirklich freiwillig. Auf den zweiten Blick ist ein gehärteter Browser jedoch auch hier nützlich, denn viele dieser „Telefonszenarien“ basieren darauf, dass der Anrufer bereits Informationen über das Konto oder den Kunden gesammelt hat. Er weiß zum Beispiel von der letzten Überweisung oder er kennt Anmelde-name und PIN. Diese eigentlich geheimen Sicherheitsmerkmale hat er vorher in einem normalen, ungeschützten Browser ausspioniert. Das verhindert Protect. Wenn Protect benutzt wird, lassen sich Sicherheitsmerkmale auf dem Kunden-PC nicht ausspionieren und damit fallen auch viele der anschließenden betrügerischen Geschäftsmodelle per Telefon ins Wasser. Auch bei einem großen Teil der klassischen Phishing-Seiten, die die Seiten der Bank nachbauen oder so tun, als handele es sich um eine spezielle Seite des Rechenzentrums, hilft der Protect-Browser. Der Kunde muss sich nur an die eine Regel halten: Bankseiten nur mit dem Protect-Browser besuchen. Das ist ähnlich wie beim Auto: erst gurten, dann spurten. Solange man die Regel einhält und „erst den Gurt klicken lässt“, ist die Sicherheit deutlich erhöht.

### **Kann Protect „als Standardbrowser“ die Links in Phishing-Mails abfangen?**

Das wäre technisch möglich, würde aber zu einem schwierigen Entscheidungsprozess führen, denn bei jedem URL-Aufruf müsste der Browser entscheiden, ob er selbst zuständig ist (die Seite einer Bank wurde geklickt) oder aber ein anderer Browser (alle sonstigen Seiten aus dem Internet). Wenn man für den zweiten Fall wieder einen anderen Browser öffnet, ist niemandem geholfen. Der Browser müsste quasi vorher wissen, ob die Seite dahinter eine gute oder eine schlechte Seite ist. Er müsste also jeden guten Internetshop und jedes gute Unternehmen sowie jede böse Seite persönlich kennen. An dieser sekundenschnellen, stets aktuellen Blacklist scheitern derzeit alle Browserhersteller von Google bis Firefox, weil die Bösen viel schneller neue Seiten ins Netz stellen, als die Guten sie erkennen können. Derzeit ist nicht geplant diesen Weg einzuschlagen.

**Kann Protect auf beliebig vielen Endgeräten genutzt werden?**

Ja

**Wie wird Protect wieder deinstalliert?**

Protect wird nicht installiert und muss daher auch nicht deinstalliert werden. Man kann das Programm einfach löschen und es ist verschwunden. Alle Daten die Protect im Benutzer-Verzeichnis angelegt hat sind verschlüsselt. Das betrifft auch die abgespeicherte PIN-Nummer, falls Sie die Funktion Autologin aktiviert haben sollten. Wenn Sie auch die verschlüsselten Benutzerdaten in Windows von Hand löschen möchten, gehen Sie bitte in das Verzeichnis „C:\Users\\AppData\Local und löschen den Ordner „CORONIC“

**Wird eine Schulung oder ein Handbuch für die Nutzung von Protect benötigt?**

Es gibt ein Endkunden-Handbuch für das Produkt. Protect verhält sich wie ein ganz normaler Browser und kann daher problemlos von jedermann verwendet werden. Für die Mitarbeiter in der Bank wird ein Supporthandbuch für Bankmitarbeiter zur Verfügung gestellt.

**Fragen zur Nutzung von S-Protect in der der Sparkassen-Finanzgruppe**

**Unterstützt Protect die neuen web-Portale der FI?**

Ja, alle. Ganz grundsätzlich gilt: Alles was in einem modernen Browser funktioniert, funktioniert auch in Protect. Daher werden alle neuen Web-Anwendungen wie Online-Terminvergabe, Online-Chat und Firmenkundenportal unterstützt.

**Kann man den Browser für den Endkunden verpflichtend machen?**

( z. B. über die OBV-Steuerung)

Das ist technisch problemlos möglich. Bei anderen Banken haben wir diese Verpflichtung im Einsatz („Protect-only“). Der Endkunde kann dann nur Online-Banking machen, wenn er auch Protect benutzt. So charmant diese Lösung technisch auf den ersten Blick wirkt, so selten wird sie jedoch benutzt. Nur 3 unserer Kunden haben dieses Feature verwendet. Es entstehen manchmal Support-Probleme. Z. B. wenn der Kunde unerwartet krank wird, im Urlaub ist oder auf Besuch bei Freunden und Verwandten dringend eine Überweisung machen muss, während der PC mit dem Browser zu Hause steht. Um ein ausschließendes Protect-only-Feature zu implementieren, muss eine Schnittstelle zur FI programmiert werden. Wenn genügend Sparkassen eine solche Funktion wünschen, versucht CORONIC ein Umsetzungsprojekt zu starten. Sparkassen können aber schon heute bei jeder Überweisung sehen, mit welchem Browser-Agent diese erfolgt ist. Protect verwendet seinen eigenen Browser-Agent und ist daher bei allen Überweisungen als sicherer Browser erkennbar.

**Wird die Arbeit über SEVA in der FI-Umgebung unterstützt?**

Ja, Protect unterstützt grundsätzlich alles, was auch normale Browser unterstützen.

**Was bewirkt die Verknüpfung „Gehärteter Browser“ im OB-Teilnehmervertrag?**

Eine solche Verknüpfung ist bereits vorhanden, da auch die FI darüber nachdachte, einen gehärteten Browser einzuführen. Die Verknüpfung ist daher noch im Auswahlmenü zu sehen. Die Funktion dahinter ist allerdings nicht aktiv. Bitte melden Sie sich gerne bei uns, wenn Sie Interesse an einer solchen Verknüpfung haben. Wenn sich genügend Sparkassen eine solche Funktion wünschen, versuchen wir ein Umsetzungsprojekt zu starten.

**Muss der Content für die IF selber eingebaut werden oder gibt es zentralen Content?**

CORONIC stellt sämtlichen Content für die Internetfiliale bereit. Schauen Sie sich als Beispiel gerne die Umsetzung der Sparkasse am Niederrhein an: <https://www.sparkasse-am-niederrhein.de/protect>. Alle dort verwendeten Grafiken, Texte und Videos finden sich auch auf unserer Infoseite: [www.coronic.de/spkinfos/#auslieferung](http://www.coronic.de/spkinfos/#auslieferung).

**Funktioniert der Browser auch mit dem Firmenkundenportal?**

Ja, Protect unterstützt grundsätzlich alles, was auch normale Browser unterstützen.

**Werden fremde Content-Inhalte in der IF vom Browser ignoriert?**

Protect zeigt alle ihm bekannten Inhalte an (Whitelist). Falls Sparkassen nicht standardkonforme Seiten oder aber auch Tools, Inhalte oder Videos von Dritten auf Ihrer Homepage einsetzen, geben Sie dem CORONIC Support gerne Bescheid und wir erweitern die Whitelist, sodass alles perfekt angezeigt wird. Nur als Beispiel: Sollten Sie heute ein Video von einer uns unbekanntem Internetseite in die Homepage einbauen, würde der Protect Browser dieses Video ausblenden, weil es nicht auf seiner Whitelist enthalten ist. Der Endkunde sieht das Video nicht, kann aber normal und ohne Fehlermeldung weiterarbeiten.

**Gibt es Probleme, wenn Sparkassen Cobra-Inhalte in der IF einsetzen?**

Nein, Protect unterstützt grundsätzlich alles, was auch normale Browser unterstützen.

**Woher bekommen Sie die Zahl der aktiven Online-Banking Kunden**

Die Zahl fragen wir zum Ende des Jahres für die Rechnungsstellung bei Ihnen an. Sie können die Zahl selbst ermitteln oder in der IF Statistik abrufen unter:

<https://statistik.sparkassen-finanzportal.de>



**Gibt es bei Druck der Erstzugangsdaten Informationen für die Endkunden über S-Protect?**

Ja, das ist möglich. Allerdings muss das jede Sparkasse für sich selbst entscheiden, ob der Standard-Druck angepasst werden soll.

**Weitere Fragen zu Protect?**

Kontakt beim Hersteller, der CORONIC GmbH

frank.bock@coronic.de

0431 530 237 - 0

[www.coronic.de/spkinfos](http://www.coronic.de/spkinfos)