Sicherheit

UC eBanking prime

Sicherheitsinformationen

unicreditgroup.eu/clientsolutions

UniCredit

Inhalt

ALLGEMEINES ZU UC EBANKING PRIME

UC eBanking prime ist eine Software die auf einem, vom Kunden zur Verfügung gestellten, Server installiert wird. Der Zugriff auf diesen Server erfolgt über einen Browser. Die Anmeldung in der Applikation erfolgt über einen separat zu installierenden OTC Client.

CLIENTKOMMUNIKATION

Die Kommunikation zwischen Client und Server sollte mittels https erfolgen. Die dafür benötigten Zertifikate müssen durch den Kunden bereitgestellt oder erzeugt werden, da diese einen privaten geheimen Schlüssel voraussetzen. Für die einfache Einrichtung stellt die UniCredit ein SSL-Tool incl. Anleitung zur Verfügung.

Wir empfehlen dabei explizit den Einsatz von Zertifikaten, welche durch ein öffentliches oder kundeneigenes Trustcenter signiert sind.

Alternativ unterstützt UC eBanking prime weiterhin http.

SICHERE SCHLÜSSELABLAGE

Die Schlüssel, die zur Anmeldung in UC eBanking prime benötigt werden, werden als Softwareschlüssel in Dateien gespeichert. Die Schlüssel sind mit einem Passwort geschützt.

Es muss unbedingt darauf geachtet werden, dass diese sicher aufbewahrt, gespeichert und vor unberechtigtem Zugriff geschützt sind. Beachten sie zudem folgende weitere Hinweise:

- Bei Schlüsseldateien, die auf einem zentralen Speichermedium abgelegt sind, können andere Personen möglicherweise Zugriff haben (z.B. Systemadministratoren).
- Wechselmedien, die Schlüsseldateien enthalten, können versehentlich offen liegen gelassen werden bzw. bleiben versehentlich im PC stecken.
- Schlüsseldateien können unbemerkt kopiert werden und so in unbefugte Hände geraten. Softwareschlüssel sollten Sie daher nicht auf stationären Datenträgern (lokales Laufwerk, Netzwerklaufwerk) ablegen, sondern zumindest auf Wechseldatenträgern speichern, die nach der Nutzung sicher zu verwahren sind. UC eBanking prime hat darüber hinaus Mechanismen implementiert, welche sicherstellen, dass immer nur mit einer Version (Original) der Schlüsseldatei gearbeitet werden kann. Die parallele Nutzung einer zweiten Version (Kopie) ist nicht möglich.
- Das Sicherheitsmedium (z.B. USB-Stick), auf dem die Softwareschlüssel gespeichert sind, ist vor missbräuchlicher Nutzung und Diebstahl zu schützen. Dieses erfordert eine sichere Aufbewahrung, z.B. durch Einschließen. Darüber hinaus empfehlen wir Ihnen, den Zugriff auf das Sicherheitsmedium zusätzlich abzusichern. Dieses kann z.B. durch den Einsatz eines speziellen USB-Sticks mit Zahlentastatur und Verschlüsselungshardware erfolgen.
- Sicherheitsmedien zur Speicherung der Schlüsseldateien sollten nur für diesen Zweck Verwendung finden und nicht noch zur Speicherung anderer Daten genutzt werden. Der Zugriff sowohl auf das Medium als auch auf die dort gespeicherten Softwareschlüssel muss durch ein Passwort abgesichert werden. UC eBanking prime erlaubt den Zugriff auf die Schlüssel nur durch Eingabe eines entsprechenden Passwortes. Regeln zur Erstellung und Änderung von Passwörtern sollten Bestandteil Ihrer unternehmensinternen Sicherheitsrichtlinie sein. Weitere Hinweise zum Thema Passwort finden Sie weiter unten in diesem Dokument.
- Nutzen sie die Möglichkeit des Schlüsselwechsels. Hierbei wird die Schlüsseldatei modifiziert und eine alte Version ist nicht mehr verwendbar.
- Nach letztmaliger Verwendung sollten die Sicherheitsmedien sicher entsorgt bzw. zerstört werden.
- UC eBanking prime bietet die Möglichkeit, das Speichern von Softwareschlüsseln ausschließlich auf externen Medien zu erlauben, sowie den User auf die Entfernung des Mediums nach der Benutzung hinzuweisen.

SOFORTIGE SPERRUNG VON SCHLÜSSELN BEI VERDACHT AUF MISSBRAUCH BZW. DIEBSTAHL

Bei Verdacht auf Missbrauch bzw. Diebstahl ist unverzüglich angeraten, Ihre Banken vom Missbrauch der Schlüssel bzw. des Verlustes/Diebstahls zu unterrichten und den EBICS-Zugang Ihrer betroffenen Nutzer mit UC eBanking prime sperren zu lassen.

EINDEUTIGE ZUORDNUNG DER SICHERHEITSMEDIEN, AUF DENEN DIE SOFTWARESCHLÜSSEL GESPEICHERT SIND

Jedem Mitarbeiter, der UC eBanking prime nutzt, muss ein eigenes Sicherheitsmedium (z. B. USB-Stick) zugeordnet sein, für das er Sorge zu tragen hat. Dieses Medium sollte der Teilnehmer ausschließlich zur Speicherung der Schlüsseldateien für UC eBanking prime verwenden.

SICHERES PASSWORT

Generell sollten Passwörter ausreichend lang und komplex sein. Ein Wechseln von Passwörtern ist zwingend notwendig, wenn Sie den Verdacht haben, dass jemand Kenntnis von Ihrem Passwort hat. Es sollten keine identischen Passwörter für unterschiedliche Zwecke oder Zugänge verwendet werden. Die Passwörter sollten sich nicht nur durch die Änderung einer Stelle des Passwortes unterscheiden.

In UC eBanking prime können Administratoren Regeln für die Zusammensetzung und Gültigkeit von Passwörtern vorgeben. Des Weiteren lässt sich die Verwendung bisheriger Passwörter einschränken.

Eine Orientierung bietet hier die Empfehlung des BSI zum Umgang mit Passwörtern: https://www.bsi-fuer-buerger.de/

Zur Vermeidung des Ausspähens von Passwörtern dürfen diese nicht im Klartext auf dem System (z.B. in einer Datei) oder auf einem Passwortzettel abgelegt werden. Stattdessen könnte ein am Markt erhältliches Programm zur Schlüsselverwaltung genutzt werden, das in der Regel auch die Generierung sicherer Passwörter erlaubt. Darüber hinaus könnte auch ein Programm zur sicheren Eingabe von Passwörtern verwendet werden, dass die Passworteingabe unter Umgehung der Tastatur erlaubt. Auf diese Weise kann verhindert werden, dass die über die Tastatur eingegebenen Passwörter von Unbefugten aufgezeichnet (mittels sogenannter Keylogger) und missbräuchlich verwendet werden.

In UC eBanking prime wird der letzte Login, bzw. Log in-Versuch angezeigt, dies sollte immer überprüft werden.

ANMELDUNG UND AUTORISIERUNG MITTELS OTC CLIENT

Um eine sichere und komfortable Anmeldung im UC eBanking prime zu ermöglichen, stellen wir Ihnen mit Installation einen so genannten OTC Client bereit. Hierbei handelt es sich um eine Software, die auf jedem Rechner, welcher UC eBanking prime nutzt, installiert werden muss. Dafür sind keine Adminrechte notwendig.

Der Client erzeugt auf Basis des Keybag und des dazugehörigen Passwortes (s.o.) einen Anmeldecode welcher 60 Sekunden gültig ist und (vergleichbar einer TAN) im Browser eingetragen werden muss. Der OTC Client baut daraufhin eine dauerhafte Verbindung zum Server auf.

Liegen Daten zum Unterschreiben vor, öffnet sich der OTC Client und zeigt die zu signierenden Daten an. Die Unterschrift wird dann wieder mittels dem o.g. Passwort geleistet. Sind alle notwendigen Unterschriften geleistet, wird die Zahlung automatisch an die Bank versendet.

AUTOMATISCHER LOG-OUT

Wird der OTC Client oder der Browser geschlossen, wird der User automatisch aus UC eBanking prime abgemeldet. Außerdem erfolgt eine automatische Abmeldung, wenn die durch den Kunden zu definierende Zeit für Inaktivität abgelaufen ist. Der User kann sich anschließend direkt wieder anmelden.

AUTOMATISCHE USERSPERRE

User die mehrfach in Folge ihr Passwort falsch eingegeben haben (die Anzahl kann durch den Kunden definiert werden) oder eine Kopie Ihres Schlüssels verwenden, werden automatisch gesperrt. Die User können dann im 4 Augenprinzip innerhalb der Software wieder entsperrt werden. Einer der User muss dabei mindestens die Rolle „Audit“ besitzen.

OPTIONALES ONE-TIME-PASSWORT (OTP)

UC eBanking prime bietet die optionale Möglichkeit zusätzlich zur Schlüsseldatei ein Einmalkennwort einzusetzen. Hierfür erzeugt ein Kennwortgenerator auf Anforderung (Empfehlung hierfür ist der Einsatz einer Smartphone App) ein Passwort welches nur einmal bzw. für eine begrenzte Zeit (z.B. 30 Sekunden) gültig ist und bei der Anmeldung und vor jeder Zahlungsfreigabe eingegeben werden muss.

UC eBanking prime unterstützt die standardisierten Verfahren TOTP und HOTP.

ZEITBESCHRÄNKTER SYSTEMZUGANG

Der Zugang zu UC eBanking prime kann für jeden User individuell zeitlich eingeschränkt werden, um den Zugang zum System bspw. nur in den Geschäftszeiten zu ermöglichen. (z.B. Montag – Freitag, 8-17 Uhr).

BERECHTIGUNG INNERHALB VON UC EBANKING PRIME

UC eBanking prime bietet ein umfangreiches Rechtesystem – es kann durch Sie individuell eingestellt werden, welche User welche Daten sehen und welche Rechte die User bekommen.

ROLLEN

Die wichtigsten Rollen, die UC eBanking prime unterscheidet, sind:

BANKING

Der User hat Zugriff auf die bankfachlichen Funktionen und Daten der Software. (bspw. Zahlungen und Kontoauszüge)

ADMIN

Der User darf bankfachliche Daten administrieren (bspw. Berechtigungen, User, Banken, Konten). Für die Administration kann außerdem durch den Administrator des Kunden das 4 Augenprinzip aktiviert werden.

SYSTEM

Der User darf technische Einstellungen vornehmen (bspw. Proxy, Organisationen).

AUDIT

Beinhaltet alle Sicherheitsrelevanten Optionen (bspw. Passworteinstellungen, Login).

Wir empfehlen fachliche und administrative Rollen strikt zu trennen.

Darüber hinaus gibt es einen Hauptadministrator für Supportmitarbeiter der Bank. Das Passwort dieses Users läuft alle 24h ab und kann nur durch einen sich täglich ändernden Einmalcode zurückgesetzt werden, welchen nur die UniCredit Bank kennt.

SICHERHEIT DES RECHNERS

SICHERES BETRIEBSSYSTEM

Das Betriebssystem und weitere installierte Software, wie z. B. PDF-Reader oder Browser, müssen regelmäßig aktualisiert werden. Dies sollte nur über die vom Softwareanbieter zur Verfügung gestellten Updatewege erfolgen, wie z. B. Windowsupdate oder die in der Software verfügbaren Aktualisierungswege.

SICHERER BROWSER

Verwenden Sie ausschließlich einen von der UniCredit Bank AG freigegebenen Browser (siehe mit der Software ausgelieferte Release Notes) und führen Sie die vom Hersteller dafür zur Verfügung gestellten Sicherheitsupdates zeitnah durch. Auf die Nutzung von Zusatzprogrammen im Browser sollte verzichtet werden, sofern diese nicht benötigt werden. Zusatzprogramme im Browser sollten nur für vertrauenswürdige Webseiten aktiviert werden. Sind in dem zu verwendenden Browser Mechanismen zum Phishing- und Malware-Schutz integriert, so sollten diese auch genutzt werden.

Hinweise zu Sicherheitseinstellungen verschiedener Browser finden sich unter www.bsi.bund.de/ .

AKTUELLER VIRENSCANNER

Der Einsatz einer Antiviren-Software ist unumgänglich. Auch diese Software ist regelmäßig zu aktualisieren. In der Regel verfügt die Antiviren-Software über einen Automatismus, so dass diese permanent im Hintergrund läuft und für eine Aktualisierung unmittelbar nach dem Start des Rechners sorgt. In regelmäßigen Abständen sollte der Rechner einer vollständigen Prüfung durch die Antiviren-Software unterzogen werden.

Achten Sie darauf, dass die verwendete Antiviren-Software den verwendeten Browser schützt.

UPDATES VON UC EBANKING PRIME

UC eBanking prime sollte regelmäßig aktualisiert werden. Wir informieren Sie über reguläre Updates und dringend notwendige (Sicherheits-)Patches über die integrierte Benachrichtigungsfunktion. Bitte prüfen Sie regelmäßig, ob hier Nachrichten für Sie vorliegen und spielen Sie die Updates zeitnah ein.

KOMMUNIKATION ZWISCHEN SERVER UND BANK

Die Kommunikation mit der Bank erfolgt ausschließlich über den Server per EBICS Standard. Die Spezifikation des Standards ist öffentlich verfügbar unter www.ebics.de und setzt neben einer starken 2.048 Bit Verschlüsselung auf TLSv1.2/TLSv1.3 als Transportverschlüsselung.

Die Kommunikation erfolgt immer ausgehend über Port 443 und kann aus Sicherheitsgründen über einen Proxy geroutet werden. Es müssen keine eingehenden Ports geöffnet werden und der Server muss nicht in der DMZ stehen oder per Internet erreichbar sein.

SOFTWAREVERTEILUNG REGELT PROGRAMMINSTALLATION

Die Installation und Pflege von Software sollte ausschließlich im Rahmen eines geregelten Prozesses erfolgen (z. B. zeitweilige Vergabe von Administratorrechten und Dokumentation). Zur Erhöhung der Sicherheit sollte die Genehmigung und Durchführung der Installation im Vieraugenprinzip erfolgen und protokolliert werden. Für die Installation und Wartung benötigte Arbeitsplätze und Zugangswege (z. B. für Fernwartungssoftware) sollten vorab definiert und genehmigt werden.

EINZELUNTERSCHRIFTEN

Aus rechtlicher Sicht ist eine Einzelzeichnung der bankfachlichen Signatur möglich, was bedeutet, dass nur eine Signatur zum Ausführen von Aufträgen erforderlich ist.

Zur Erhöhung der Sicherheit empfehlen wir den Einsatz einer gemeinschaftlichen Zeichnung. Hierbei vereinbaren Sie mit der Bank, dass zwei oder mehrere Signaturen für die vollständige Autorisierung erforderlich sind. Dieses 4-Augen Prinzip ist ein wirksamer Schutz gegen Angriffe, da eine böswillig eingefügte oder manipulierte Zahlung (bspw. nach Verlust oder Diebstahl des Schlüssels aber auch nach Social-Engineering-Angriffen), durch den 2. Unterschreibenden erkannt und verworfen werden kann.

VERANTWORTUNGSBEWUSSTER UMGANG MIT DATEN UND PROGRAMMEN

Treffen Sie Maßnahmen zur Informationssicherheit auf organisatorischer, technischer und personeller Ebene. Hierzu gehören u.a. Zugangs- und Zugriffsschutz, Installation von Firewalls, Berechtigungsmanagement sowie Monitoring und Protokollierung. Der Schutz vor Schadsoftware ist in der heutigen Zeit unverzichtbar.

Darüber hinaus sollten Sie einen geregelten Prozess zur Installation von Software und Vorkehrungen zum Schutz des Unternehmensnetzwerkes treffen.

Damit die enthaltenen Sicherheitsverfahren zum Schutz der ausgetauschten Daten Ihre volle Wirkung entfalten können, sind aber auch in Ihrer technischen Umgebung entsprechende Vorkehrungen erforderlich. Hinweise und insbesondere aktuelle Meldungen zur Basissicherheit finden sich unter www.bsi.bund.de .

SICHERE SCHNITTSTELLEN ZWISCHEN UC EBANKING PRIME UND IHREM ERP SYSTEM

UC eBanking prime bietet die Option Ordner zu definieren, welche regelmäßig (i.d.R. zwischen 3 und 5 Minuten) abgefragt werden und alle darin befindlichen Zahlungsdateien importiert. Außerdem können abgerufene Daten (bspw. Kontoauszüge) für eine Weiterverarbeitung in definierte Ordner gelegt werden.

BERECHTIGUNGEN FÜR SCHNITTSTELLEN

Es dürfen nur User berechtigt werden, welche Dateien erzeugen und in die Schnittstellen von UC eBanking prime ablegen müssen, bzw. die dort abgelegten Auszüge abholen dürfen. Generell empfehlen wir, wenn möglich, dass nur die Hostsysteme (Server UC eBanking prime und Server ERP System) auf die Schnittstellen zugreifen können. Für diesen Zweck empfiehlt es sich, einen ADS User zu definieren, welcher auf den Ordner berechtigt ist und der als Context beim UC eBanking prime Tomcat Dienst für diesen Zweck hinterlegt wird.

HASH-WERTE

UC eBanking prime kann bei der Anzeige der Zahlungsverkehrsdateien die Hash-Werte im SHA256 oder MD5 Verfahren mit anzeigen. Damit kann der Benutzer überprüfen, ob der Hash-Wert aus dem ERP-System dem entspricht, welchen UC eBanking prime errechnet hat. Dadurch können nachträgliche Manipulationen an Zahlungsdateien aus ERP Systemen wirkungsvoll verhindert werden.

Hierfür muss das ERP-System diese Informationen an den Benutzer übermitteln z. B. durch Andruck auf Begleitdokumenten. Eine erfolgreiche Nutzung dieser Funktion setzt voraus, dass in beiden Systemen über die identische Methode der Hash generiert wird.

Wir empfehlen den Einsatz eines SHA256 Hashwertes.

VERSCHLÜSSELUNG

UC eBanking prime kann über die automatischen Schnittstellen Dateien importieren, welche mit AES256 verschlüsselt wurden.

Es wird eine AES/ECB/PKCS5Padding-Verschlüsselung mit einem 256Bit Schlüssel verwendet. Grundlage des Schlüssels ist der SHA256-Hash eines durch den Kunden definierten Passwortes („PreSharedKey“). Dieses wird einmal definiert und nicht fortlaufend geändert. Das Passwort wird im UC eBanking prime hinterlegt und kann nur mit Adminrechten geändert werden.

Wir empfehlen eine Verschlüsselung immer in Kombination mit der Anzeige des Datei-Hash-Wertes zu kombinieren (s.o.).

FAKTOR MENSCH

Von Social Engineering spricht man immer dann, wenn ein Angreifer menschliche Eigenschaften ausnutzt, um an vertrauliche Informationen zu kommen. Internetkriminelle sind in der Vorstellung vieler Menschen technisch versierte Genies, die komplexe Computercodes programmieren, um damit in fremde Computernetzwerke einzudringen. Dies entspricht jedoch häufig nicht der Realität. Neben dem klassischen „Hacken“, also dem Eindringen mit technischen Mitteln wie z.B. Computerviren, gibt es für Kriminelle auch einen einfacheren Weg an die gewünschten Informationen zu gelangen.

Warum nicht einfach nett danach fragen? Kaum zu glauben, aber die Methode des „Social Engineerings“ verspricht insbesondere in Unternehmen mit überdurchschnittlichen IT-Sicherheitsvorkehrungen große Erfolge für den Angreifer.

Angreifer nutzen dazu menschliche Eigenschaften der Mitarbeiter wie z.B. Gutgläubigkeit, Hilfsbereitschaft, Stolz, Konfliktvermeidung oder Respekt vor Autoritäten aus, um mit psychologischen Tricks an die gewünschten Informationen zu gelangen. Ein Social-Engineering-Angriff beginnt in der Regel mit der Beschaffung von allgemeinen Informationen über das Unternehmen, das angegriffen oder ausspioniert werden soll.

Social Engineering ist für Internetkriminelle ein beliebtes Mittel, um unberechtigt an sensible Informationen zu gelangen: Es kostet nichts und überwindet selbst die besten sicherheitstechnologischen Barrieren.

Schon ein Organigramm und die Telefonliste können einem versierten Angreifer genügen. Dieser ruft nun in dem Wissen um die vorherrschenden hierarchischen Strukturen beim Unternehmen an. Er täuscht eine falsche Identität vor, um sich durch eine geschickte Fragestellung und mit psychologischen Mitteln langsam an die Zielinformation heranzutasten. Häufig schlüpft der Täter in die Rolle einer Autoritäts- oder Vertrauensperson. Dabei sammelt er Informations-Puzzlesteine, die ihn an anderer Stelle als vertrauenswürdig erscheinen lassen.

Besonders häufig haben es Social Engineers auf Passwörter, z.B. die Zugangsdaten zu Bankdaten abgesehen. So täuscht der Angreifer beispielsweise ein Problem vor, das einer sofortigen Lösung bedarf, z.B. ein Hackerangriff, der sofortigen Zugriff auf den Bank-Account erfordert. Weil er bestimmt und autoritär auftritt, sein Opfer zuvor unter psychologischen Gesichtspunkten ausgewählt hat und es zusätzlich mit Stress konfrontiert, gibt ihm dieses oftmals bereitwillig die Zugangsdaten heraus.

Social Engineers geben sich als jemand aus, der sie in Wirklichkeit nicht sind und täuschen so eine Identität vor. Erteilen Sie daher keine Auskünfte, zu denen Sie nicht ausdrücklich ermächtigt worden sind. Das gilt für die Arbeits- und Betriebsorganisation, Zuständigkeiten, persönliche Informationen von Kollegen oder gar Benutzerdaten. Geben Sie nur so viele Informationen preis wie nötig und hinterfragen Sie ungewöhnliche Anliegen eines Anrufers.

Leichtsinnige Entscheidungen in punkto Sicherheit werden insbesondere in Stresssituationen oder aus Höflichkeit getroffen. Im Zweifelsfall gilt Sicherheit vor Höflichkeit. Mit Ihrem Vorgesetzten sollten Sie absprechen, dass Ihnen keine Nachteile daraus entstehen, wenn Sie sich bei Unsicherheit rückversichern und der Vorstand oder ein wichtiger Kunde eine Weile auf das gewünschte Dokument warten muss.

Bewahren Sie schriftliche Notizen und Briefverkehr niemals auf Ihrem Schreibtisch auf, sondern schützen Sie diese Informationen vor den Blicken Dritter. Speichern Sie sensible Dokumente stets verschlüsselt auf Ihrem PC. Selbst aus scheinbar unwichtigen Informationen können im Zusammenspiel mit anderen wichtige Schlüsse gezogen werden. Vermeiden Sie es, an öffentlichen Plätzen wie im Zugabteil oder im Café über sensible Unternehmensinterna zu sprechen.

Weitere Informationen zum Thema Social Engineering und aktuelle Beispiele finden Sie auf unserer eigens dafür eingerichteten Website: http://www.hvb.de/ceo-fraud

ZERTIFIZIERUNG

UC eBanking prime wird jährlich durch TÜV Trust IT geprüft. Das Prüfungszertifikat stellen wir Ihnen für die aktuelle Version auf Anforderung gern bereit.

SUPPORT

Beim Verdacht, dass:

- Jemand unautorisiert Zugriff auf Ihr Konto hat oder hatte
- Ihr Zugang verloren gegangen ist, gestohlen oder kopiert wurde
- Sie Opfer eines CyberCrime Angriffes geworden sind

oder aber Sie Fragen zur Sicherheit im Allgemeinen oder zu diesem Dokument haben, dann kontaktieren Sie bitte umgehend unseren Helpdesk unter:

TELEFON +49 89 55299699

ODER

PER EMAIL GTB-CENTER@UNICREDIT.DE

UniCredit Bank AG
Client Solutions

Address
Arabellastr. 14
81925 München

Contact
Transaction & Payments Support
+49 89 55 299 699

Online
gtb-center@unicredit.de
ebanking.unicreditgroup.de