Sicherheit

Corporate Portal

Sicherheitsinformationen

hilfe.hvb.de
gtb-center@unicredit.de

UniCredit

Inhalt

ALLGEMEINES ZU CORPORATE PORTAL

SICHERES PASSWORT

SICHERHEIT DES RECHNERS

ZWEI FAKTOR AUTHENTIFIZIERUNG

- UC MOBILE TOKEN APP
- PHOTO TAN

EINZELUNTERSCHRIFTEN

VERANTWORTUNGSBEWUSSTER UMGANG MIT DATEN UND PROGRAMMEN

MOBILE ENDGERÄTE

SOFTWAREVERTEILUNG REGELT PROGRAMMINSTALLATION

FAKTOR MENSCH

BESONDERHEITEN FÜR EINZELNE ANWENDUNGENUC

- UC EBANKING GLOBAL
- UC TRADER
- UC TRADE FINANCE GATE
- COMMUNICATION SUITE

SUPPORT

ALLGEMEINES ZU CORPORATE PORTAL

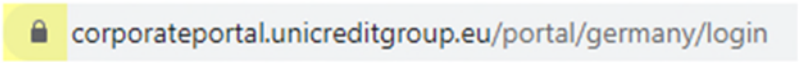
Im Gegensatz zu einer auf Ihrem lokalen Rechner betriebenen Software, handelt es sich bei Corporate Portal um ein Angebot, das bei der UniCredit zentral für eine Vielzahl von Kunden betrieben wird. Der Zugriff auf Corporate Portal erfolgt über einen Browser, wobei alle Funktionalitäten in diesem Browser dargestellt werden. Sämtliche Daten – mit Ausnahme des geheimen Schlüssels – liegen nicht lokal bei Ihnen.

Wie allgemein üblich, sollte auch für Corporate Portal und alle damit verbundenen Anwendungen eine regelmäßige Überprüfung und Anpassung der Berechtigungsprofile auf Aktualität (z.B. Löschen ausgeschiedener Mitarbeiter, Änderung von Zeichnungsberechtigungen etc.) erfolgen. Sofern Sie für den Corporate Portal Zugang ein besonders hohes Schutzniveau für erforderlich erachten, sollte der Zugang nur einem eingeschränkten Personenkreis gewährt werden.

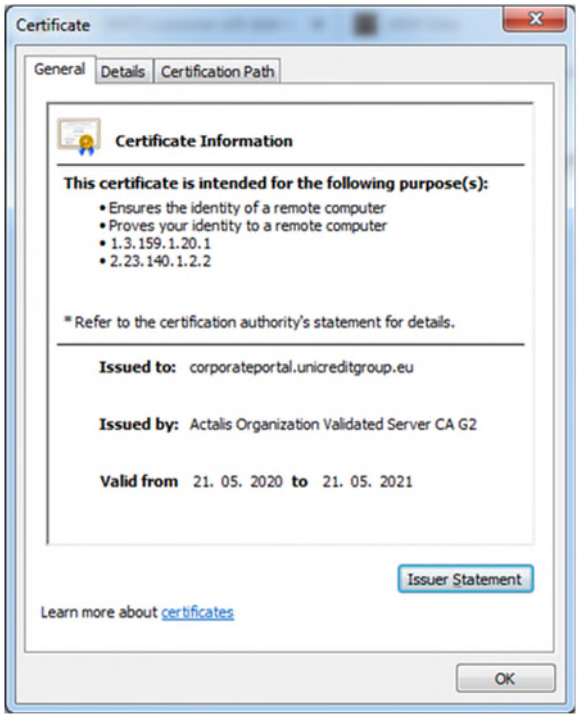
AUFRUF VON CORPORATE PORTAL

Die Datenkommunikation zwischen Kunde und Bank findet über eine per TLS verschlüsselte https-Kommunikation statt. Die meisten Browser signalisieren Ihnen eine gesicherte https-Kommunikation in dem z.B. ein „Schloss-Symbol“ im Browser angezeigt wird. Geben Sie vertrauliche Daten (insbesondere Ihr Passwort) niemals ein, ohne zuvor die Adresse zu kontrollieren! Unten sehen Sie ein Beispiel aus dem Chrome Browser von Google.

https://corporateportal.unicreditgroup.eu/portal/germany/login



Das Zertifikat muss für den Betreiber der Portal-Lösung (im Falle von Corporate Portal die UniCredit Bank) ausgestellt sein. Es ist von einer vertrauenswürdigen Zertifizierungsstelle signiert. Um sicherzugehen, dass Sie tatsächlich mit der gewünschten Adresse verbunden sind, haben Sie die Möglichkeit, das Serverzertifikat zu überprüfen. Klicken Sie dazu doppelt auf das „Schloss-Symbol“ in der Browser-Statusleiste.



Es darf zu keinen Zertifizierungsproblemen bei dem Aufruf der Internet-Adresse von Corporate Portal kommen. In diesen Fällen warnt der Browser und weist auf ein Problem mit dem Sicherheitszertifikat hin, bzw. gibt den Hinweis, dass dieser Verbindung nicht vertraut wird. Kontaktieren Sie dann bitte unseren Helpdesk unter Telefon +49 89 55299699 oder per Email gtb-center@unicredit.de

Die notwendige Internetverbindung zur Nutzung von Corporate Portal sollte grundsätzlich über einen gesicherten Internet-Zugang hergestellt werden. Von einer Nutzung ungesicherter oder unbekannter WLAN-Zugänge (z. B. Internetcafé) ist dringend abzuraten.

SINGLE SIGN ON

Wenn Sie sich erfolgreich im Corporate Portal angemeldet haben, stehen Ihnen alle Ihnen zugeordneten Applikationen ohne weitere Anmeldung direkt zur Verfügung („Single Sign On“).

Die Nutzung der weiteren Anwendungen (und damit verbunden die Zuordnung zu Ihrem Login) erfordert in der Regel einen weiteren Vertrag, dafür wenden Sie sich bitte an Ihren Spezialisten oder Ihren Betreuer.

Sollte eine Applikation eine weitere Autorisierung erfordern (bspw. Transaktionen), so erfolgt dies ebenfalls mit dem für den Login genutzten Sicherheitsmedium.

AUTOMATISCHER LOG-OUT

Aus Sicherheitsgründen erfolgt nach 5 Minuten Inaktivität ein automatischer Log-Out. Sie können sich danach sofort wieder anmelden.

Einzelne Anwendungen können darüber hinaus einen längeren Log-Out haben.

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 auch nicht nur durch die Änderung einer Stelle des Passwortes unterscheiden.

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

An Stellen, wo ein Passwort notwendig ist, bedingt Corporate Portal oder die damit verbundene Applikation eine Mindestqualität an Passwörter, die bei der Vergabe des Passwortes automatisch geprüft wird. Diese Mindestregeln werden durch die Bank vorgegeben und können sich, wenn erforderlich, ändern.

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 Passwortverwaltung genutzt werden, das in der Regel auch die Generierung sicherer Passwörter erlaubt.

SICHERHEIT DES RECHNERS

SICHERES BETRIEBSSYSTEM

Das Betriebssystem und weitere installierte Software, wie z. B. PDF-Reader und 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 freigegebenen Browser (siehe Release Notes) und führen 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.

ZWEI FAKTOR AUTHENTIFIZIERUNG

Die Zwei-Faktor-Authentifizierung dient der Authentifizierung eines Users mittels zweier voneinander unabhängiger Merkmale. So kann diese min. 2 Faktor Authentifizierung aus den Merkmalen „Wissen“ (bspw. Passwort), „Besitz“ (Besitz des Smartphones, photoTAN Readers oder der Schlüsseldatei) und „Biometrie“ (bspw. Fingerabdruck, Face-ID) kombiniert sein.

UC MOBILE TOKEN APP

AUTHENTIFIZIERUNG UND AUTORISIERUNG MIT SMARTPHONES

Die UC Mobile Token App ist eine vollständige Sicherheitsanwendung, die die erforderlichen privaten Schlüssel für die Benutzerauthentifizierung und für die Autorisierung von Transaktionen, wie Zahlungen oder administrativen Modifikationen bereithält und damit auf einen zusätzlichen Kanal verlagert. Nur wenn der User im Besitz des Smartphones und des zugehörigen Passwortes und/oder biometrischen Merkmal ist, kann er mit Corporate Portal arbeiten.

EINLOGGEN MIT DER UC MOBILE TOKEN APP

Für die Anmeldung am Corporate Portal nutzt der Anwender oder der Administrator sein Smartphone, auf dem er die UC Mobile Token App heruntergeladen und eingerichtet hat. Corporate Portal zeigt dem Benutzer einen Zugangscode an, den er in die App auf seinem Smartphone eingibt bzw. per QR Code abscannt. Er wird jetzt zur Eingabe eines sicheren Passwortes (s.o. Passwortsicherheit) aufgefordert. Optional kann der User biometrische Merkmale (Face-ID, Touch-ID) zur Authentifizierung nutzen. Nachdem das System den Code überprüft hat, kann der Benutzer sicher mit Corporate Portal arbeiten.

SICHERHEIT DER UC MOBILE TOKEN APPS

Alle Apps der UniCredit Bank erkennen Modifikationen durch Jailbreaks oder Root-Kits und werden daher aus Sicherheitsgründen umgehend alle in der App gespeicherten Daten und Schlüssel löschen.

Die Daten der UC Mobile Token App sind mit einem gerätespezifischen Merkmal verschlüsselt. Daher sind diese an das eingesetzte Smartphone gebunden. Bei einem Gerätewechsel muss die App neu eingerichtet werden und das neue Smartphone durch das alte autorisiert werden. Eine Anleitung dazu finden Sie auf unserer Hilfeseite.

Nach fünfmaliger aufeinanderfolgender fehlerhaften Passworteingabe löschen die UC Mobile Token Apps ebenfalls alle in der App gespeichert Daten.

Die UC Mobile Token Apps erfordern immer auch, dass ein Gerätepasswort oder eine biometrische Gerätesperre vergeben ist. Ist dies nicht der Fall, können die Apps nicht eingerichtet werden.

DOWNLOAD DER UC MOBILE TOKEN APPS

Google Play Store für Android:

https://play.google.com/store/apps/details?id=de.unicredit.mobiletoken&hl=de

Apple App Store für iPhone:

https://apps.apple.com/de/app/uc-mobile-token/id1103148048

PHOTOTAN

AUTHENTIFIZIERUNG UND AUTORISIERUNG MIT PHOTOTAN

Das photoTAN Verfahren ist ein sicheres 2 Faktor Verfahren welches einen photoTAN Generator erfordert und auch dann eingesetzt werden kann, wenn kein Smartphone für die Nutzung des UC Mobile Token zur Verfügung steht. Nur wenn der User im Besitz des jeweiligen photoTAN Gerätes ist und die PIN kennt, kann er mit Corporate Portal arbeiten.

Auf einem photoTAN Generator können bis zu 8 Zugänge gespeichert werden. Dabei wird für jeden User eine individuelle PIN vergeben.

EINLOGGEN MIT DEM PHOTOTAN GERÄT

Das Lesegerät dient der Erstellung eines individuellen TAN-Codes. Für die Anmeldung benötigen Sie Ihre Portal ID, das zugeordnete photoTAN Geräte sowie eine frei wählbare mindestens 4-stellige PIN.

Zukünftig wird Ihnen bei jedem autorisierungspflichtigen Vorgang die photoTAN Grafik, ein quadratisches Bild mit bunten Punkten, angezeigt. Diese Grafik scannen Sie einfach mit Ihrem photoTAN Lesegerät und geben danach Ihre PIN ein. Sie erhalten dann auf dem Display Ihres photoTAN Lesegerätes die für diesen Vorgang gültigen Daten zum Abgleich. Nach Bestätigung generiert das Gerät die notwendigen TAN, welche Sie dann im Corporate Portal eingeben.

SICHERHEIT DES PHOTOTAN GERÄTES

Die Daten sind mit Ihrer PIN geschützt. Nach fünfmaliger aufeinanderfolgender fehlerhafter PIN-Eingabe, löscht der photoTAN Generator den Zugang und der User muss sich neu initialisieren.

BESTELLUNG DES PHOTOTAN GENERATORS

Eine Bestellung ist unter http://www.hvb.de/order-phototan möglich

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 enthalten 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 http://www.bsi.bund.de/ .

MOBILE ENDGERÄTE

Täglich werden neue Schwachstellen in der Software und den Betriebssystemen von Smartphones und Tablets entdeckt. Diese können von Angreifern ausgenutzt werden und stellen damit eine Gefahr für Ihr Gerät dar. Um sich zu schützen, müssen Sie das Betriebssystem und die Anwendungen immer auf dem neuesten Stand halten, Aktualisierungen einpflegen oder neuere Programmversionen installieren. Dabei den Überblick zu behalten, ist oft eine Herausforderung. Für Ihr mobiles Endgerät gelten grundsätzlich die gleichen Regeln, wie für Ihre Computer.

Das größte Sicherheitsrisiko ist der Verlust Ihres Smartphones. Vergeben Sie daher ein Passwort für eine Bildschirmsperre oder nutzen Sie zusätzliche Sicherheitsmechanismen. So können Unbefugte nicht auf Ihre Anwendungen und Daten zugreifen. Ändern Sie bei dem Verlust Ihres Smartphones am besten alle Passwörter und nutzen Sie die Möglichkeit mittels eines Sicherheitsprogrammes per Fernzugriff Ihre Daten auf dem Smartphone zu löschen bzw. das Gerät zu sperren.

Lassen Sie Ihr Smartphone nie unbeaufsichtigt, wenn Sie Ihr Corporate Portal geöffnet haben. Achten Sie auch darauf, dass Ihnen niemand über die Schulter schaut, wenn Sie sensible Daten eingeben. Nutzen Sie Ihr mobiles Gerät für Ihre Bankgeschäfte nur in vertrauenswürdigen WLAN-Umgebungen oder über Ihre mobile Datenverbindung.

Laden Sie Apps nur aus vertrauenswürdigen Quellen wie etwa Apple App Store oder Google Play Store. Kontrollieren Sie trotzdem bei den dort heruntergeladenen Apps die Datenschutzeinstellungen, Zugriffsrechte und ggfs. weitere externe Bewertungen. Schränken Sie ggf. ihre Sicherheitsrichtlinie auf die aktuellen Rahmenbedingungen ein.

Seien Sie vorsichtig bei Links, die Sie per SMS oder E-Mail erhalten. Dies gilt auch für Links, die sich hinter QR-Barcodes verstecken. Folgen Sie Links nur, die aus vertrauenswürdigen Quellen stammen.

Deaktivieren Sie den Internetzugang, Bluetooth, Infrarot sowie WLAN und NFC, wenn Sie diese nicht nutzen. So erschweren Sie Kriminellen den Zugriff auf Ihre Daten über WLAN -Spots und Bluetooth. Verschlüsseln Sie am besten Ihre Daten und deaktivieren Sie zudem die Gerätekennung über Bluetooth.

Sichern Sie Ihre Daten regelmäßig auf einem gesicherten, stationären Gerät. Wenn Sie Ihr mobiles Gerät verkaufen, verschenken oder entsorgen, löschen Sie vorher die Daten.

Jeder Hersteller bietet für seine Betriebssysteme regelmäßig Service- und Sicherheitsupdates an. Informieren Sie sich auf den Webseiten Ihres Herstellers.

Die Kommunikation zwischen Ihrem mobilen Endgerät und Ihrer Bank arbeitet äußerst stabil. Systemabbrüche oder Ähnliches sind sehr selten. Seien Sie daher misstrauisch, wenn Ihr mobiles Endgerät sich ungewöhnlich verhält. Insbesondere, wenn es zu Abbrüchen oder Fehlermeldungen nach Eingabe des Passwortes kommt. Im Zweifelsfall nehmen Sie Kontakt mit Ihrem Kreditinstitut auf.

Verzichten Sie auf die Installation von Modifikationen des Smartphone Betriebssystems („Jailbreak“, „Custom-ROMs“ oder „Rootkit“). Diese Modifikationen können Code enthalten, welche es Angreifern erlaubt den Datenverkehr der eBanking Apps mitzulesen.

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). Insbesondere im Falle der Installation von Bank-Software durch Fremd-dienstleister sollten für die Installation spezielle technische Zugänge genutzt werden, die nach der Installation wieder deaktiviert werden sollten. Diese technischen Zugänge sollten vorab durch den IT-Verantwortlichen Ihres Unternehmens genehmigt werden. Zur Erhöhung der Sicherheit sollte die Genehmigung und Durchführung der Installation im 4-Augen Prinzip erfolgen und protokolliert werden. Für die Installation und Wartung benötigte Arbeitsplätze und Zugangswege (z. B. für Fernwartungssoftware) sollten vorab definiert und genehmigt werden.

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

BESONDERHEITEN FÜR EINZELNE ANWENDUNGEN

UC EBANKING GLOBAL

UC eBanking global ist eine eBanking Applikation, mit der Sie Auszüge empfangen und Zahlungen erfassen und versenden können und unterliegt damit der PSD2 Richtlinie. Es ist vollständig im Corporate Portal integriert. Alles für das Corporate Portal geschriebene gilt auch für UC eBanking global, zusätzlich gibt es noch folgende weitere Sicherheitsmerkmale:

ZAHLUNGEN UND MODIFIKATIONEN MIT DER UC MOBILE TOKEN APP AUTORISIEREN

Um Zahlungen oder administrative Modifikationen im UC eBanking global zu autorisieren, wählt der Benutzer die Objekte aus, die er freigeben will. Automatisch zeigt die UC Mobile Token App eine Zusammenfassung dieser Auswahl auf dem Smartphone des Benutzers an. Der Benutzer kann dies überprüfen, und ganz bequem durch die Eingabe seines Passworts oder per Touch-ID autorisieren. Anschließend sendet UC eBanking global der Bank die Transaktionen zur weiteren Verarbeitung, wenn alle erforderlichen Unterschriften vorhanden sind.

Dieses Verfahren ist auch für eingerichtete EBICS Drittbanken nutzbar.

ZAHLUNGEN UND MODIFIKATIONEN MIT PHOTOTAN AUTORISIEREN

Um Zahlungen oder administrative Modifikationen im UC eBanking global zu autorisieren, wählt der Benutzer die Objekte aus, die er freigeben will. Der User scannt mit dem photoTAN Geräte die angezeigte Grafik und erhält eine Zusammenfassung dieser Auswahl auf dem Gerät angezeigt. Der Benutzer kann dies überprüfen und bekommt nach Bestätigung und Eingabe seiner PIN eine TAN angezeigt. Diese gibt er im UC eBanking global ein. Anschließend sendet UC eBanking global der Bank die Transaktionen zur weiteren Verarbeitung, wenn alle erforderlichen Unterschriften vorhanden sind.

Schlüsseldateien im Falle von Fremdbanken in Verbindung mit photoTAN

Sollen weitere EBICS Drittbanken genutzt werden, muss hier – zur Wahrung der Kompatibilität mit dem EBICS Standard – zusätzlich weiterhin ein Keybag.dat Schlüssel genutzt werden.

Diese Schlüssel werden als Softwareschlüssel in Dateien gespeichert. Die Schlüssel sind hier zusätzlich mit einem Passwort geschützt.

Achten Sie unbedingt darauf, dass diese sicher aufbewahrt und gespeichert und vor unberechtigtem Zugriff geschützt sind.

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.

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 Zahlen-tastatur 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 global 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 in dieser Broschüre.

Nach letztmaliger Verwendung sollten die Sicherheitsmedien sicher entsorgt bzw. zerstört werden.

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 Zugang Ihrer betroffenen Nutzer zu UC eBanking global sperren zu lassen.

Sie haben zusätzlich jederzeit die Möglichkeit des Schlüsselwechsels. Hierbei wird ihr Schlüssel modifiziert und eine alte Version ist nicht mehr verwendbar.

UC TRADER

Beim UC Trader erfolgt kein Log Out der Anwendung nach 5 Minuten Inaktivität. Ihre Anmeldung im Corporate Portal oder anderen Anwendungen wird aber weiterhin nach 5 Minuten Inaktivität beendet.

Für weitere Fragen zum UC Trader wenden Sie sich bitte an Ihren Corporate Treasury Sales Spezialisten oder an den FX eSales Support.

UC TRADE FINANCE GATE

Beim UC Trade Finance Gate erfolgt kein Log Out der Anwendung nach 5 Minuten Inaktivität. Diese Toleranz für Inaktivität bis zum Log Out beträgt hier 30 Minuten. Ihre Anmeldung im Corporate Portal oder anderen Anwendungen wird aber weiterhin nach 5 Minuten Inaktivität beendet. Sie können aber unabhängig davon weiter im UC Trade Finance Gate arbeiten und Transaktionen übertragen.

Die Administration der Rechte für Benutzer erfolgt teils durch die Bank (Anlage von Nutzern mit Freigaberechten), teils durch die vom Kunden benannten Hauptnutzer. Die Erfassungs-, Lese- und Freigaberechte werden über Benutzerrollen definiert, die sich nach der gewählten UC Trade Finance Gate Edition bestimmen. Einzelheiten hierzu entnehmen Sie bitte den im UC Trade Finance Gate zur Verfügung gestellten Handbüchern oder wenden Sie sich an Ihren Trade Finance Spezialisten.

COMMUNICATION SUITE

Über die Communication Suite des Corporate Portals können Sie sicher Nachrichten und Dateien mit der UniCredit austauschen. Im Gegensatz zur E-Mail-Kommunikation erfolgt eine Transportverschlüsselung. Darüber hinaus können einzelne Nachrichten und Dateien mit einer Signatur versehen werden, welche in bestimmten Fällen eine Unterschrift ersetzen kann.

Stimmen Sie sich hierfür bitte bilateral mit Ihrem Spezialisten oder Betreuer ab.

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:

GTB-CENTER@UNICREDIT.DE