Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Electronic Banking Internet Communication Standard (EBICS)

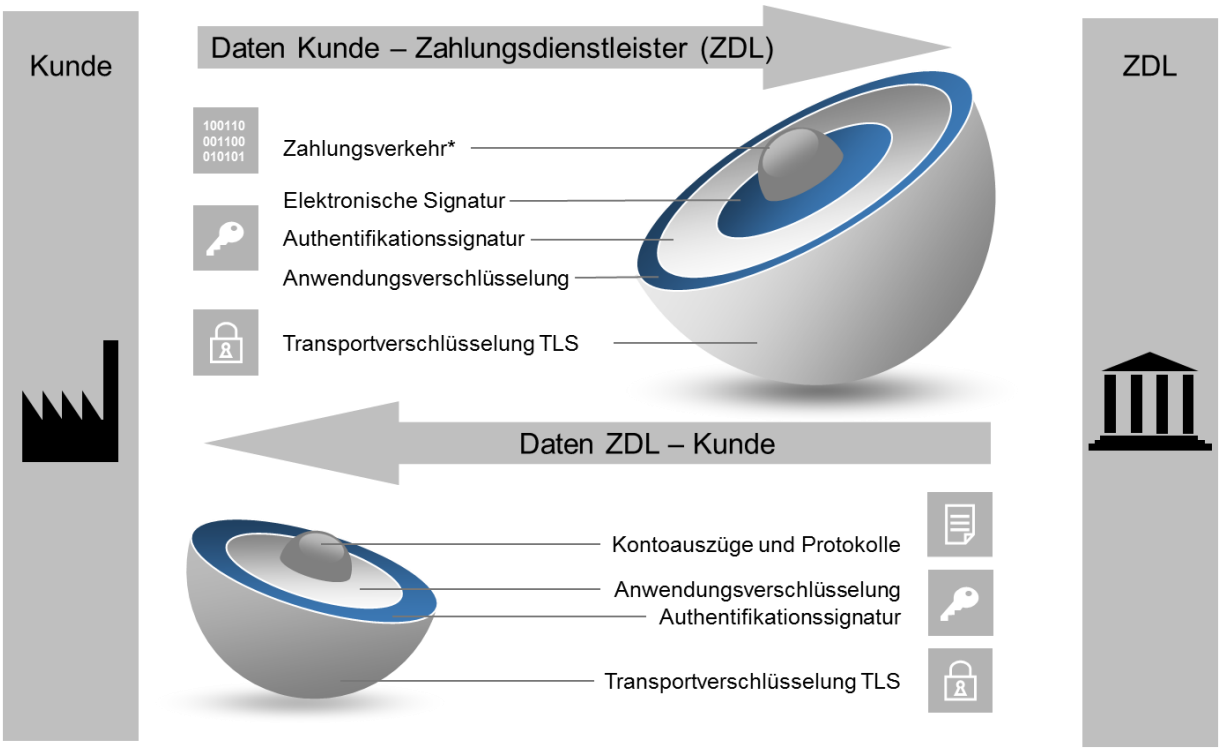
Sicherheitsempfehlungen für Firmenkunden

Stand: 3. September 2018

Inhalt

1 Einleitung

Der Electronic Banking Internet Communication Standard (EBICS) hat sich als multibankfähiges und hochsicheres Kommunikationsverfahren zwischen Ihnen und Ihrem Zahlungsdienstleister seit Jahren bewährt. Mehrfache Verschlüsselung der bankfachlichen Daten, unterschiedliche elektronische Signaturen, sowie ein umfassendes Berechtigungsmanagement für Nutzer bilden dabei die Basis für die EBICS Sicherheitsarchitektur, die durch die folgende Abbildung illustriert werden soll:



* Auch andere Dateiformate möglich

Der Transport Ihrer Zahlungsverkehrsdaten an Ihren Zahlungsdienstleister wird durch doppelte Verschlüsselung und zwei Signaturen abgesichert: Die Elektronische Signatur/Unterschrift unterschreibt die fachlichen Daten (Autorisierung), während die Authentifikationssignatur sicherstellt, dass Sie der richtige Sender sind (Authentifizierung). Mit der Anwendungsverschlüsselung werden Ihre Zahlungsverkehrsdaten verschlüsselt. Während des Transportes ist der gesamte Datenstrom (also auch weitere Steuerdaten) zusätzlich durch eine TLS[1]-Verschlüsselung geschützt. Insbesondere raten wir, gemäß

[1] Transport Layer Security

Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) die Verwendung von TLS 1.2 für die EBICS-Transportverschlüsselung mit den im Rahmen von TLS 1.2 unterstützten und empfohlenen „Cipher-Suiten“[2].

Ihr Zahlungsdienstleister liefert Ihnen Daten zur Abholung mit den gleichen Sicherheitsmechanismen. Eine bankseitige Elektronische Unterschrift (EU) für diese Daten ist technisch in EBICS möglich, jedoch durch die Finanzbehörden noch nicht durchgängig anerkannt. Daher wird zurzeit noch auf diese EU verzichtet.

Die Deutsche Kreditwirtschaft[3] sowie auch die EBICS-Gesellschaft[4] überprüfen regelmäßig die eingesetzten Sicherheitsmechanismen und Verschlüsselungstechniken auf Aktualität, um dieses hohe Sicherheitsniveau aufrecht zu erhalten.

Dies ist insbesondere durch die sich permanent verändernde und sich verschärfende Bedrohungslage im Internet unerlässlich. Die rapide steigende Anzahl von Schadsoftware und immer raffiniertere Angriffstechniken sowie die zunehmende organisierte Kriminalität machen dies nötig.

Damit die im EBICS 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 www.bsi.bund.de.

Dieses Dokument richtet sich an alle Kunden, die EBICS nutzen, insbesondere an Firmenkunden und deren IT-Abteilungen, Sicherheitsverantwortliche und Systemadministratoren. Es beschreibt Bedrohungen, die in spezifischen Implementierungsvarianten vorhanden sind und gibt Empfehlungen, wie diesen begegnet werden kann.

---

[2] Empfehlungen zu EBICS-Sicherheitsverfahren und Schlüssellängen der Deutschen Kreditwirtschaft http://www.ebics.de/index.php?eID=tx_securedownloads&u=0&g=0&t=1530525352&hash=83900c86833e899302b51e931f60e74c3f21a19c&file=/fileadmin/user_upload/2015-12-21-EBICS-Sicherheitsempfehlungen.pdf

[3] Die Deutsche Kreditwirtschaft (kurz DK) ist als Zusammenschluss des Bundesverbandes der Deutschen Volksbanken und Raiffeisenbanken, des Bundesverbandes deutscher Banken, des Bundesverbandes Öffentlicher Banken Deutschlands, des Deutschen Sparkassen- und Giroverbandes und des Verbandes deutscher Pfandbriefbanken die Interessenvertretung der kreditwirtschaftlichen Spitzenverbände. Sie ist im August 2011 hervorgegangen aus dem Zentralen Kreditausschuss (ZKA) und führt dessen Arbeit fort.

[4] Mitglieder der EBICS-Gesellschaft sind die Kreditwirtschaften Deutschlands, Frankreichs und der Schweiz.

Das Dokument hat Empfehlungscharakter und erhebt keinen Anspruch auf Vollständigkeit.

In Kapitel 2 („Allgemeine Maßnahmen zur Absicherung“) gibt dieses Dokument generelle Sicherheitsempfehlungen. Hier werden Hinweise auf die Einrichtung einer Sicherheitsorganisation, eines Sicherheitsmanagements sowie exemplarisch einige Tipps zur Absicherung von Netzwerken gegeben.

In Kapitel 3.1 („Der Schutz für Ihre Elektronische Unterschrift“) geht dieses Dokument auf Risiken und Bedrohungen beim Schlüsselmanagement ein und gibt insbesondere Hinweise zur sicheren Speicherung Ihrer Schlüssel.

Anschließend werden in Kapitel 3.2 („Nutzung von Portal-Lösungen“) die spezifischen Risiken bei der Nutzung von Portal-Lösungen betrachtet und entsprechende Maßnahmen zur Vermeidung dieser Risiken dargestellt.

Der zunehmenden Nutzung mobiler Endgeräte – entweder für den Einsatz von EBICS-Apps oder als Medium im Rahmen der verteilten elektronischen Unterschrift (VEU), trägt Kapitel 3.3 („Nutzung von Tablets, Smartphones und Phablets“) Rechnung. Hier wird insbesondere auf die besonderen Bedrohungen bei Nutzung von Smartphones und Tablets etc. eingegangen und Empfehlungen für Sicherheitsmaßnahmen für diese Plattformen gegeben.

Da Social-Engineering-Angriffe als zunehmendes Element bei unterschiedlichsten Arten von Identitätsdiebstahl – auch durch die immer stärkere Nutzung von Sozialen Netzwerken und der damit einhergehenden Preisgabe von persönlichen und dienstlichen Informationen - eine immer stärkere Rolle spielen, wird diesem Thema ein eigenes Kapitel in diesem Dokument gewidmet (Kapitel 3.4).

2 Allgemeine Maßnahmen zur Absicherung

Die DFÜ-Kundenbedingungen, die Sie von Ihrem Zahlungsdienstleister ausgehändigt bekommen haben, stellen eine Minimalanforderung dar. Sie können Ihre Sicherheit aber noch weiter optimieren.

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, wie beispielsweise:

- 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 der EBICS-Software durch Fremddienstleister 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 Vieraugenprinzip erfolgen und protokolliert werden. Für die Installation und Wartung benötigte Arbeitsplätze und Zugangswege (z. B. für Fernwartungssoftware) sollten vorab definiert und genehmigt werden.

- Wie allgemein üblich sollte auch für EBICS eine regelmäßige Überprüfung und Anpassung der Berechtigungsprofile auf Aktualität (z. B. Löschen ausgeschiedener Mitarbeiter, Änderung von Zeichnungsberechtigungen etc.) erfolgen.

- Sofern Sie für den EBICS-Client ein besonders hohes Schutzniveau für erforderlich erachten, sollte der Betrieb zur Gewährleistung der Sicherheit auf einem dedizierten, abgesicherten, stationären Endgerät erfolgen. Dies können Sie z. B. erreichen, indem nur ein eingeschränkter Personenkreis Zugang zum EBICS-Client erhält.

- Das Betriebssystem und weitere installierte Software sollte regelmäßig aktualisiert werden (Installation von Patches).

- 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. Fehlt ein solcher Automatismus, so sollte die Antiviren-Software grundsätzlich nach jedem Start des Rechners und vor dem Start des EBICS-Systems manuell aktualisiert werden. In regelmäßigen Abständen sollte der Rechner einer vollständigen Prüfung durch die Antiviren-Software unterzogen werden.

- Generell sollten Passwörter ausreichend lang sein und Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Ein regelmäßiges Wechseln von Passwörtern wird empfohlen. Es sollten keine identischen Passwörter für unterschiedliche Zwecke oder Zugänge verwendet werden.

- Zur Vermeidung des Ausspähens von Passwörtern dürfen diese nicht im Klartext auf dem System (z. B. in einer Datei) 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, das 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[5]) und missbräuchlich verwendet werden.

- In der Regel wird von Electronic Banking-Produkten (EBICS-Clients und -Portalen) der letzte Login, bzw. Login-Versuche angezeigt, dies sollte immer überprüft werden, achten sie hierbei auf fehlerhafte Login-Versuche.

- Die für eine EBICS-Kommunikation notwendige Internetverbindung sollte grundsätzlich über einen gesicherten Internet-Zugang hergestellt werden. Von einer Nutzung ungesicherter oder unbekannter WLAN-Zugänge (z. B. Internetcafé) ist dringend abzuraten.

[5] Ein Keylogger ist eine Hard- oder Software, die die Tastatureingaben eines Benutzers an einem Computer protokolliert, überwacht oder rekonstruiert. Mittels Keylogger können z. B. Passwörter, die ein Benutzer über die Tastatur eingibt, mitgelesen und einem Angreifer unbemerkt zur Verfügung gestellt werden.

3 Risiken und mögliche Bedrohungen

3.1 Der Schutz für Ihre Elektronische Unterschrift

3.1.1 Wo liegen die potenziellen Risiken?

Die in EBICS definierten Sicherheitsverfahren für die Authentifizierung, Verschlüsselung und Autorisierung von Zahlungsaufträgen (Elektronische Unterschrift) bieten einen sehr hohen Schutz vor betrügerischen Manipulationen und unberechtigter Einsichtnahme in die vertraulichen Daten im Electronic Banking.

Alle diese Verfahren basieren auf sog. asymmetrischen Verschlüsselungsverfahren, bei denen jeweils mit einem privaten Schlüssel Signaturen zur Authentifizierung von EBICS-Nutzern und zur Autorisierung von Aufträgen erstellt werden. Umgekehrt werden mit öffentlichen Schlüsseln die Signaturen geprüft und Daten verschlüsselt. Daher ist es von besonderer Wichtigkeit, dass die privaten und öffentlichen Schlüssel sicher aufbewahrt und vor unberechtigtem Zugriff und (unbemerkten) Veränderungen geschützt sind. Unbefugte Personen, die im Besitz einer Kopie der Schlüssel und des zugehörigen Passwortes oder PIN sind, können unter falscher Identität Aufträge einreichen und autorisieren, gegebenenfalls Einsicht in die Kontoinformationen erlangen und Aufträge manipulieren.

Die Schlüssel können entweder auf spezieller Hardware (Chipkarten), im Rahmen eines Fernsignaturverfahrens oder als Softwareschlüssel in Dateien gespeichert sein. In der Regel bieten Zahlungsdienstleister ihren Kunden Chipkarten an, die eine erhöhte Sicherheit bieten. Die Schlüssel sind hier zusätzlich mit einer PIN, einer persönlichen Identifikationsnummer, geschützt. Aus Sicherheitsgründen empfehlen wir Ihnen die Speicherung der Schlüssel auf Chipkarten, da diese weder unbemerkt kopiert bzw. entwendet noch ohne Kenntnis der PIN verwendet werden können.

Sollten Sie dennoch Schlüsseldateien[6] verwenden, sollten Sie unbedingt darauf achten, dass diese sicher aufbewahrt und gespeichert und vor unberechtigtem Zugriff geschützt sind.

Insbesondere sollten Sie die folgenden Risiken bei der Verwendung von Schlüsseldateien beachten:

- Die Schlüsseldateien können unbemerkt durch Schadsoftware zusammen mit den Passwörtern an einen Angreifer geleitet werden.
- Bei Schlüsseldateien, die auf einem zentralen Speichermedium abgelegt sind, können andere Personen möglicherweise Zugriff haben (z. B. Systemadministratoren).

[6] Sofern kein Hardwaremedium z. B. Chipkarte verwendet wird, sind die Schlüssel in Schlüsseldateien abgelegt und werden dann Softwareschlüssel genannt.

- Wechselmedien, die Schlüsseldateien enthalten, können versehentlich offen liegen gelassen werden bzw. bleiben versehentlich im PC stecken.

3.1.2 Welche Maßnahmeempfehlungen leiten sich daraus ab?

Sichere Speicherung von Softwareschlüsseln

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 Zahlentastatur und Verschlüsselungshardware erfolgen.

Sofortige Sperrung von Schlüsseln bei Verdacht auf Missbrauch bzw. Diebstahl

Bei Verdacht auf Missbrauch bzw. Diebstahl ist unverzüglich angeraten, Ihre Zahlungsdienstleister vom Missbrauch der Schlüssel bzw. des Verlustes/Diebstahls zu unterrichten und den DFÜ-Zugang Ihrer betroffenen Nutzer mit EBICS-Mitteln (Auftragsart SPR) zu sperren.

Eindeutige Zuordnung der Sicherheitsmedien, auf denen die Softwareschlüssel gespeichert sind

Jedem Mitarbeiter, der als EBICS-Teilnehmer das EBICS-Kundensystem 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 das EBICS-Verfahren verwenden.

Regelmäßiges Wechseln der verwendeten Schlüsseldateien

Bei Verwendung von Schlüsseldateien empfehlen wir Ihnen den regelmäßigen Wechsel der Schlüssel in bestimmten Zeitintervallen. Vorgaben zum Schlüsselwechsel sollten Bestandteil Ihrer unternehmensinternen Sicherheitsrichtlinie sein.

Der EBICS-Standard bzw. die EBICS-Clientsoftware bietet entsprechende Funktionalitäten zum Update der verwendeten Schlüsseldateien.

Verwendung geeigneter Sicherheitsmedien zur Speicherung von Schlüsseldateien und Verwendung geeigneter Passwörter für den Zugriff auf die Softwareschlüssel

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. In der Regel erlaubt bereits die verwendete EBICS-Software den Zugriff auf die Schlüssel nur durch Eingabe eines entsprechenden Passwortes. Regeln zur Erstellung und Änderung von Passwörtern sollten Bestandteil Ihrer unternehmensinternen Sicherheitsrichtlinie sein. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt Tipps für sichere Passwörter unter www.bsi.bund.de.

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

Erhöhung der Sicherheit durch Mehr-Augen-Prinzip

Aus rechtlicher Sicht ist eine Einzelzeichnung der bankfachlichen Signatur möglich, zur Erhöhung der Sicherheit wird seitens der Deutschen Kreditwirtschaft eine gemeinschaftliche Zeichnung empfohlen. Hierbei vereinbaren Sie mit dem Zahlungsdienstleister, dass zwei Signaturen für die vollständige Autorisierung erforderlich sind.

3.2 Nutzung von Portal-Lösungen

3.2.1 Wo liegen die potenziellen Risiken?

Im Gegensatz zu einem auf einem lokalen Rechner betriebenen EBICS-System handelt es sich bei einer Portal-Lösung um ein Angebot, das bei dem Zahlungsdienstleister oder einem Service-Provider zentral für eine Vielzahl von Kunden betrieben wird.

Der Zugriff auf die Portal-Lösung erfolgt über einen Browser, wobei sämtliche Funktionalitäten des EBICS-Systems in diesem Browser dargestellt werden. Sämtliche Daten – mit Ausnahme des geheimen Schlüssels bei einer Verwendung von Schlüsseldateien – liegen nicht lokal bei Ihnen. Konkret sind die EBICS-Schlüssel für Authentifizierung und Verschlüsselung sowie sämtliche bankfachliche Daten (Zahlungsaufträge, Kontoauszüge, etc.) in der Umgebung des Betreibers der Portal-Lösung gespeichert.

Neben der Eingabe von Benutzerkennung und Passwort kann zusätzlich die Eingabe einer weiteren Kennung erforderlich sein, die der Betreiber des Portals per SMS an eine zuvor definierte Mobilfunknummer versendet.

Für die Verwendung der Schlüssel gelten insbesondere auch die in Kapitel 3.1 „Der Schutz für Ihre Elektronische Unterschrift“ aufgezeigten Risiken. Die dort empfohlenen Maßnahmen zur Minimierung der Risiken sollten Sie unbedingt befolgen.

Bei der Nutzung von Portal-Lösungen sind folgende Risiken zu beachten:

- Durch die Verwendung eines Browsers stehen Portal-Lösungen grundsätzlich im Fokus von Schadsoftware. Diese kann unter bestimmten Umständen eine Manipulation von Zahlungsverkehrsdaten durchführen oder Einsichtnahme in sensiblen Daten (z. B. Kontoinformationen) erreichen.

- Auf Grund eines angegriffenen Browsers könnten die benötigten Zugangsdaten zum Portal in die Hände von Dritten geraten.

3.2.2 Welche Maßnahmeempfehlungen leiten sich daraus ab?

Verwendung freigegebener Browser

Verwenden Sie ausschließlich einen vom Zahlungsdienstleister freigegebenen Browser 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. Dies gilt vor allem für Java-Anwendungen, die durch zusätzliche PlugIns[7] bereitgestellt 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. Das BSI gibt Tipps für sichere Web-Browser unter https://www.bsi.bund.de.

Verwendung von Antiviren-Software

Achten Sie darauf, dass die verwendete Antiviren-Software den verwendeten Browser schützt. Um sich zu schützen, müssen Sie die Software immer auf dem neuesten Stand halten, Aktualisierungen einpflegen oder neuere Programmversionen installieren.

Gesicherter Zugang zu der Portal-Lösung

Bei der Nutzung einer Portal-Lösung werden Ihre Daten (z. B. eine erfasste Zahlung) zwischen dem Browser auf Ihrem Computer und dem Portal übertragen. Diese Daten sollten ausschließlich verschlüsselt übertragen werden. Der Betreiber einer Portal-Lösung muss zur Verschlüsselung hierbei das TLS-Protokoll einsetzen, damit eine sichere Netzverbindung zwischen Browser und dem Portal aufgebaut wird.

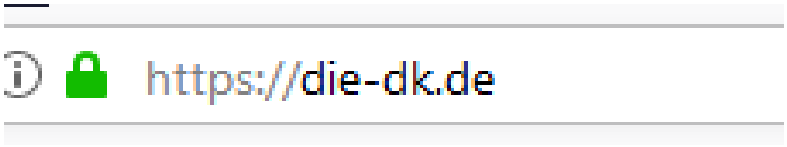
Das TLS-Protokoll gewährleistet, dass Daten während der Übertragung nicht eingesehen oder manipuliert werden können.

Zum Aufbau einer verschlüsselten Verbindung muss die Portal-Lösung über eine URL verfügen, die mit dem Kürzel **https** (und nicht http) beginnt.

Die meisten Browser helfen Ihnen hierbei in dem z. B. ein „Schloss-Symbol“ im Browser angezeigt wird. Geben Sie vertrauliche Daten (insbesondere Ihren PIN-Code und das Passwort) niemals ein, ohne zuvor die Adresse zu kontrollieren!

[7] Ein **Plugin** (auch **Software-Erweiterung** oder **Zusatzmodul**) ist eine optionale Software-Komponente, die eine bestehende Software erweitert bzw. verändert.

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



Prüfung von Zertifikaten

Das Zertifikat muss für den Betreiber der Portal-Lösung 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 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. In diesem Fall schließen Sie bitte unverzüglich die Anwendung und melden Sie den Fehler beim Kundendienst des Betreibers der Portal-Lösung.

Weitere Sicherheitsfunktionen bei der Portal-Lösung

Sollten für den Zugang zu der Portal-Lösung weitere Sicherheitsfunktionen (z. B. Zwei-Faktor-Authentifizierung[8] angeboten werden, so sollten diese auch verwendet werden.

3.3 Nutzung von Tablets, Smartphones und Phablets

Täglich werden neue Schwachstellen in der Software und den Betriebssystemen entdeckt. Diese können von Angreifern ausgenutzt werden und stellen damit eine Gefahr für Ihr Tablet, Smartphone bzw. *Phablet* dar. Um sich zu schützen, müssen Sie das Betriebssystem und

[8] Die Zwei-Faktor-Authentifizierung (2FA) dient der Authentifizierung eines Users mittels zweier voneinander unabhängiger Merkmale. So kann eine 2FA z. B. aus den Merkmalen „Wissen“ (z. B. Passwort) und „Besitz“ (z. B. Besitz einer Chipkarte) kombiniert sein.

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 Rechner.

3.3.1 Wie sichern Sie Ihr mobiles Endgerät?

Passwort

Das größte Sicherheitsrisiko ist der Verlust Ihres mobilen Endgeräts! 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 mobilen Endgeräts am besten alle Passwörter und nutzen Sie die Möglichkeit mittels eines Sicherheitsprogrammes per Fernzugriff Ihre Daten auf dem mobilen Endgerät zu löschen.

Gebrauch in der Öffentlichkeit

Lassen Sie Ihr mobiles Endgerät nie unbeaufsichtigt, wenn Sie Ihre EBICS-Anwendung 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.

Vertrauenswürdige Quellen

Laden Sie Apps nur aus vertrauenswürdigen Quellen. Kontrollieren Sie trotzdem bei den dort heruntergeladenen Apps die Datenschutzeinstellungen, Zugriffsrechte und gegebenenfalls weitere externe Bewertungen.

Werden im Unternehmen Smartphones als dienstliches Mobiltelefon eingesetzt, dann sollte eine Nutzungsvereinbarung abgeschlossen werden. Ein wichtiger Aspekt dieser Nutzungsvereinbarung ist, welche Apps auf den Geräten erlaubt oder verboten sind. Längst ist bei der Anzahl an verfügbaren Apps nicht mehr möglich, den Überblick zu behalten. Eine **Blacklist** mit verbotenen Apps ist daher schwer aktuell zu halten. Es empfiehlt sich daher eine **Whitelist** mit **vertrauenswürdigen Apps**. Doch hier stellt sich die Frage, wie die Vertrauenswürdigkeit bestimmt werden kann. Einen Anhaltspunkt für die Vertrauenswürdigkeit der Apps bietet das Projekt PrivacyGrade der Carnegie Mellon University. Dort werden Android-Apps nach dem amerikanischen Notensystem von A+ bis D bewertet. Bewertungskriterium ist dabei der Vergleich zwischen den Erwartungen der Nutzer an die Neugier der Apps mit den tatsächlichen Zugriffsrechten.

Schränken Sie Ihre Sicherheitsrichtlinie auf die aktuellen Rahmenbedingungen ein.

SMS, E-Mails, QR-Barcodes

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.

Deaktivierung nicht benötigter Dienste

Deaktivieren Sie den Internetzugang, Bluetooth, Infrarot sowie WLAN und NFC[9], 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.

Anti-Viren-Programme

Nutzen Sie ein Anti-Viren-Programm. Apps dazu finden Sie in Ihrem Store (teilweise sind diese sogar kostenlos).

Daten sichern, Daten löschen

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

Pflegen Sie das Betriebssystem Ihres Gerätes

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

3.3.2 Wie erkennen Sie Schwachstellen in Software oder Betriebssystem?

Es gibt Software zur Erkennung von Schwachstellen und zum aktuellen Softwarestand Ihrer Applikationen sowie Ihres Betriebssystems. Wir empfehlen Ihnen, diese zu nutzen.

---

[9] Die Nahfeldkommunikation (englisch *Near Field Communication*, abgekürzt NFC) ist ein auf der RFID-Technik basierender internationaler Übertragungsstandard zum kontaktlosen Austausch von Daten per elektromagnetischer Induktion mittels loser gekoppelter Spulen über kurze Strecken von wenigen Zentimetern und einer Datenübertragungsrate von maximal 424 kBit/s. Bisher kommt diese Technik vor allem im Bereich Micropayment – bargeldlose Zahlungen kleiner Beträge – zum Einsatz. Weitere Anwendungen sind beispielsweise die Übertragung von Bluetooth- oder WLAN-Authentifizierungsdaten zum Aufbau einer Kommunikation, oder das Aufrufen von Weblinks, wenn im NFC-Chip eine URL im entsprechenden Format hinterlegt wurde.

Abbruch nach Eingabe der PIN

Die Kommunikation zwischen Ihrem mobilen Endgerät und Ihrem Zahlungsdienstleister 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 einer PIN kommt. Im Zweifelsfall nehmen Sie Kontakt mit Ihrem Zahlungsdienstleister auf.

3.4 Social Engineering

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.

3.4.1 Wie geht der Angreifer vor und was sind seine potenziellen Ziele?

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 Ihr Konto 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.

Soziale Netzwerke im Internet bieten eine gute Ausgangsbasis für Social Engineering. Über diese Plattformen können eine Vielzahl von Hintergrundinformationen über Personen gefunden werden. Die Informationen, die sie über ihr Profil preisgeben, können gesammelt und als Grundlage für die weitere Informationsbeschaffung genutzt werden.

3.4.2 Was können Sie für Ihre Sicherheit unternehmen?

Sind Sie bei Auskünften zurückhaltend.

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.

Lassen Sie Sicherheit vor Höflichkeit walten.

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.

Schützen Sie sensible Informationen.

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.

Folgen Sie keinen Verweisen auf sensible Inhalte

Seien Sie besonders vorsichtig, wenn Sie unter einem dringenden oder belohnenden Vorwand auf sensible Daten zugreifen sollen. So geben sich Angreifer gerne als Ihr Chef oder Ihr Zahlungsdienstleister aus, um an sensible Informationen zu gelangen.