Sicherheit

Informationen zum Thema Sicherheit

Das Internet hat sich zu einem selbstverständlichen Medium entwickelt, dessen Bedeutung stetig zunimmt. Neben den positiven Möglichkeiten des Internets ergeben sich jedoch auch eine Reihe von Sicherheitsrisiken, denen durch geeignete Maßnahmen entgegengewirkt werden muss.
Für die Sicherheit des InternetBankings/Brokerage ist neben der Vielzahl von Sicherheitsvorkehrungen, die durch Volks- und Raiffeisenbanken und IT-Dienstleister der Banken eingeleitet wurden, die Sicherheit des Internetnutzer-PCs sowie die Sensibilisierung der InternetBanking-Nutzer von hoher Bedeutung.
Gerade aktuelle Angriffszenarien zielen immer öfter nicht nur auf die Ausnutzung von System- und Anwendungsschwachstellen und nutzen gezielt bestimmte Verhaltensmuster der Anwender. Durch den sensiblen Umgang mit den gegebenen technischen Möglichkeiten lassen sich jedoch die meisten Angriffe abwehren.

Folgende Punkte sind von wesentlicher Bedeutung:

Sicherheit am Internet-PC
Prüfung der Authentizität des Online-Angebots
Abgleich des Fingerprints (SSL-Server-Zertifikat)
Generelle Verhaltensregeln

Sicherheit am Internet-PC

Der vertrauenswürdige Zustand Ihres PCs ist die Voraussetzung für sicheres InternetBanking / Internet-Brokerage. Um die Sicherheit Ihres PCs zu gewährleisten, sind folgende Maßnahmen von wesentlicher Bedeutung:
Nutzen und installieren Sie nur Software aus vertrauenswürdigen Quellen.
Überlegen Sie immer, ob Sie eine Software wirklich brauchen und ob Sie dem Anbieter (Hersteller und Download-Quelle) wirklich vertrauen. Generell sollten Sie keine Dateien von unbekannten Servern bzw. E-Mail-Anhänge unbekannten Ursprungs öffnen, herunterladen oder ausführen. Sollte dies jedoch erforderlich sein, so ist zumindest eine Überprüfung der Dateien mit einem aktuellen Virenscanner sinnvoll.
Schutz vor Viren, Würmern und "Trojanischen Pferden"
Einmal auf Ihrem System installierte Viren, Würmer oder "Trojanische Pferde" haben auf Ihrem System weitreichende Möglichkeiten. Sobald eine solche Schadsoftware auf Ihrem System installiert wurde, kann der Schutz Ihrer Daten und die korrekte Funktion von Betriebssystem und Anwendungen prinzipiell nicht mehr gewährleistet werden.
Um eine optimale Abwehr von Schadsoftware zu erreichen, ist die Installation eines Virenscanners und einer Personal Firewall erforderlich bzw. sinnvoll. Wesentlich für die Wirksamkeit dieser Komponenten ist zudem eine regelmäßige Aktualisierung (mind. 1-mal pro Woche).

Sicherheitsaktualisierungen für Betriebssystem und Browser

Zum Teil nutzen Angreifer und Schadprogramme Sicherheitslücken im Betriebssystem und Programmen wie dem Browser, um sich unbemerkt in Ihrem PC einzunisten. Um das Angriffspotential über offene Schwachstellen zu minimieren, sollten Aktualisierungen für Betriebssysteme, Browser und Sicherheitskomponenten (wie Personal Firewall oder Virenscanner) umgehend installiert werden. Die meisten Programme bieten für diesen Zweck automatische Update-Funktionen, die in regelmäßigen Abständen auf den Herstellerseiten nach Aktualisierungen der Produkte suchen und diese ggf. installieren.

Auf folgenden Seiten finden Sie weiterführende Informationen zur Sicherheit im Internet:

www.bsi-fuer-buerger.de
www.buerger-cert.de

Prüfung der Authentizität des Online-Angebots

Die Authentifizierung ist der Nachweis eines Kommunikationspartners, dass er tatsächlich derjenige ist, für den er sich ausgibt. Die Authentizität wird beim InternetBanking / Internet-Brokerage durch Einsatz des SSL-Protokolls gewährleistet. Hierbei wird über ein Zertifikat die Authentizität des Anbieters bestätigt. Eine erste und einfache Möglichkeit der Prüfung ist zudem anhand der angezeigten Internet-Adresse (URL) im Browser möglich.
Prüfen der Internet-Adresse
Als Anwender sollten Sie darauf achten, dass Sie die korrekte Adresse (URL) für das InternetBanking / Internet-Brokerage kennen. Bei jeder InternetBanking / Internet-Brokerage Sitzung sollten Sie die im Browser angezeigte URL auf Plausibilität prüfen. Jede unbekannte Internet-Adresse kann als nicht vertrauenswürdig eingestuft werden. Geben Sie bei fremden Adressen niemals persönliche Informationen und/oder Ihre InternetBanking / Internet-Brokerage-Zugangsdaten ein.

Der Zugang zum InternetBanking / Internet-Brokerage sollte immer über die offizielle Homepage Ihrer Bank gestartet werden. Auf keinen Fall sollten Sie Links zum InternetBanking / Internet-Brokerage verwenden, die über Web-Seiten oder E-Mails anderer Anbieter zur Verfügung gestellt werden.

Bedeutung und Kontrolle der wesentlichen Bestandteile der Internet-Adresse (URL) des InternetBankings/Brokerage der Volks- und Raiffeisenbanken bei der GAD eG

Die Adresse des InternetBankings beginnt immer mit:

https:// - Kommunikation über das SSL-Protokoll (Verschlüsselte Kommunikation mit Authentizitätsnachweis des Anbieters) gad.de - Internet-Domain des IT-Dienstleisters für Volks- und Raiffeisenbanken (GAD eG) internetbanking - Name der InternetBanking-Systeme bei gad.de

Die Adresse des InternetBrokerage beginnt immer mit:

http:// - Kommunikation über das HTTP-Protokoll. Ab der Anmeldung wird für die Kommunikation das verschlüsselte HTTPS-Protokoll verwendet.

vr-networld.de - Internet Domain des Finanzportals der Volks- und Raiffeisenbanken

www.brokerage - symbolischer Ort des Service ?Brokerage?

Diese Bestandteile der URL müssen immer übereinstimmen.

Zertifikatsprüfung
Die SSL-Verbindung garantiert Ihnen, dass eine verschlüsselte Kommunikation mit der GAD eG, dem IT-Dienstleister Ihrer Volks- und Raiffeisenbank, stattfindet. SSL-Zertifikate enthalten hierfür generell den öffentlichen Schlüssel des Anbieters, sowie Angaben zur eindeutigen Identifikation.
Das SSL-Zertifikat zum InternetBanking / Internet-Brokerage ist auf den IT-Dienstleister der Volks- und Raiffeisenbanken ausgestellt (Besitzer/Antragsteller).
Hierbei handelt es sich um die GAD eG mit Sitz in Münster.
Niemals sollte ein Zertifikat eines anderen Anbieters im Rahmen einer InternetBanking / Internet-Brokerage Sitzung akzeptiert werden. Manuelle Bestätigungen des Zertifikats sind zudem beim InternetBanking / Internet-Brokerage der GAD eG nicht erforderlich, da hierbei ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle zum Einsatz kommt.
Potentielle Angreifer nutzen i.d.R. eigenerstellte Zertifikate, welche vom Browser nur mit Bestätigung des Benutzers akzeptiert werden, da dieser die Authentizität nicht zweifelsfrei feststellen kann.

Bei Zertifikatsfragen des Browsers ist daher Vorsicht geboten, bevor fremde Zertifikate akzeptiert bzw. als vertrauenswürdig eingestuft werden.

Das Zertifikat des Anbieters sowie Angaben zur Stärke der Verschlüsselung Ihrer SSL-Sitzung können Sie überprüfen, indem Sie einen Doppelklick auf das Symbol "Vorhängeschloss" in der Statuszeile des Browsers durchführen.

Zertifizierungsstelle
Die Zertifizierungsstelle ist eine international anerkannte, unabhängige und vertrauenswürdige Instanz, die Zertifikate ausstellt. Bei der Zertifikatsausstellung ist ein spezieller Authentizitätsnachweis erforderlich, so dass später über das ausgestellte Zertifikat eine Authentizitätsprüfung möglich ist.
Das InternetBanking / Internet-Brokerage der GAD eG verwendet "VeriSign" als Zertifizierungsstelle.

Als weitere Möglichkeit steht Ihnen ein Abgleich des Fingerprints des SSL-Zertifikats zur Verfügung. Beachten Sie hierzu bitte die Hinweise im folgenden Absatz.

Abgleich des Fingerprints (SSL-Server-Zertifikat)

Weitergehend können Sie die Korrektheit und Authentizität des verwendeten Zertifikats überprüfen, indem Sie den sogenannten Fingerprint (Fingerabdruck) aufrufen.
Wenn Sie die Details des Zertifikats im Browser betrachten, wird Ihnen der unten aufgeführte Fingerprint angezeigt. Durch den Abgleich der angezeigten Daten mit den Informationen des Herausgebers können Sie sicher feststellen, dass es sich um das Originalzertifikat handelt, welches Sie nutzen möchten. Das SSL-Zertifikat sichert Ihnen zu, dass eine gesicherte Kommunikation mit dem gewünschten Gesprächspartner verschlüsselt erfolgt.

Das gängigste und derzeit sicherste Verfahren zur eindeutigen Authentizitätsbestimmung ist SHA-1.
Der Fingerprint nach SHA-1 für das InternetBanking-Zertifikat (https://internetbanking.gad.de/) :

C8 42 F0 86 CF A5 A7 8C 1C 69 D1 3B 2D C7 86 4A DC B4 48 DB

Der Fingerprint für das Brokerage (https://www.brokerage.vr-networld.de/) lautet:
A8 0A 9F CA 40 F2 0E 48 C6 14 99 5C 67 BC 61 98 07 02 FF 5C

Generelle Verhaltensregeln

Geheimhaltung von PIN und TAN
PIN und TANs dürfen nur im gesicherten InternetBanking / Internet-Brokerage Angebot verwendet werden. Niemals dürfen PIN und TAN per E-Mail übertragen oder auf anderem Wege Dritten anvertraut werden.
Achten Sie darauf, dass Ihnen bei der Eingabe von PIN und TAN niemand "über die Schulter sieht" und speichern Sie nie Ihre PIN und TAN auf der Festplatte oder anderen Speichermedien Ihres PCs. Deaktivieren Sie hierzu auch die automatische Passwort-Speicherung Ihres Browsers.

Änderung der PIN bei Verdacht der Kompromittierung
Sollten Sie versehentlich eine zweifelhafte Internet-Seite besucht und Ihre Daten preisgegeben haben, empfehlen wir Ihnen, die PIN zu ändern. Dies kann im InternetBanking Angebot der Volks- und Raiffeisenbanken durchgeführt werden. Wenden Sie sich bei Problemen umgehend an Ihre Bank.
Prüfung der SSL-Verbindung
Die Stärke der Verschlüsselung Ihrer SSL-Sitzung sowie das Zertifikat des Anbieters können Sie überprüfen, indem Sie einen Doppelklick auf dem Symbol "Vorhängeschloss" in der Statuszeile des Browsers durchführen.
Nutzen Sie InternetBanking / Internet-Brokerage nur über die gesicherten SSL-Verbindungen zum Rechenzentrum der GAD eG.
Achten Sie auf die Korrektheit der InternetBanking / Internet-Brokerage-Adresse (URL).
Rufen Sie das InternetBanking / Internet-Brokerage ausschließlich über die Homepage Ihrer Volks- und Raiffeisenbank auf.

Die korrekte URL des InternetBanking beginnt immer mit .
Die korrekte URL des InternetBrokerage beginnt immer mit .
Reagieren Sie in keiner Weise auf E-Mails bzgl. InternetBanking / Internet-Brokerage, die Ihnen unaufgefordert zugestellt werden
Niemals wird eine Bank seine Kunden per E-Mail auffordern, vertrauliche Daten preiszugeben. E-Mails mit Inhalten wie: "Bitte prüfen Sie umgehend Ihren Online-Banking Zugang" weisen i.d.R. auf den Versuch

einer so genannten Phishing Attacke hin. Hierbei versuchen Betrüger, OnlineBanking-Nutzer auf ihre Web-Seite zu locken, um Zugangsinformationen zu Online-Konten zu sammeln. I.d.R. befindet sich in diesen Mails ein Link, der direkt zum InternetBanking / Internet-Brokerage führen soll. Die Internet-Adresse hat dabei meist nur marginale Abweichungen von der echten InternetBanking / Internet-Brokerage-Adresse und der optische Eindruck der echten Seiten wird vollständig nachgeahmt. Nutzen Sie daher niemals Links, die Ihnen in Mails angeboten werden.

Die Absenderadresse solcher E-Mails ist fast immer gefälscht, so dass eine Rückverfolgung dieser E-Mails sinnlos ist.

Nutzen Sie die Funktion "Abmelden" beim Beenden einer InternetBanking / Internet-Brokerage-Sitzung Erst mit dem Aufruf dieser Funktion wird Ihre Verbindung ordnungsgemäß getrennt. Die automatische Abmeldung erfolgt erst, wenn für die Dauer von 5 Minuten keine Eingaben durch den Benutzer erfolgt sind. Sie werden in diesem Fall zur Neuanmeldung aufgefordert.
Hinterfragen Sie immer kritisch, ob die auf einer Webseite geforderten Eingaben in Zusammenhang mit der von Ihnen gewünschten Aktion Sinn machen.

Versenden Sie bis zum Abmelden der InternetBanking / Internet-Brokerage-Sitzung keine E-Mails.