IT-Sicherheit im Handwerk

Checkliste IT-Sicherheit

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

TASK FORCE IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Online-Banking

Basisschutz / Sensibilisierung

Gefahr/ Risiko	Prüfung des Ist-Zustands		Maßnahme
Schadsoftware kann vorhanden sein.	Sind die Geräte, die Sie zum Online-Banking verwenden, ausreichend geschützt?	Nein →	Wenden Sie die „Checkliste Basisschutz“ an. Umgesetzt?
	Stammt die Zahlungsverkehrssoftware, der Browser bzw. die Banking-App aus einer vertrauenswürdigen Quelle und sorgen Sie für regelmäßige Updates?	Nein →	Beziehen Sie Software/Updates nicht aus unbekannten Quellen, da sie Schadsoftware enthalten könnten und somit nicht zum Online-Banking genutzt werden sollten. Beziehen Sie nur von ihrer Bank empfohlene Software/Updates aus den Originalquellen der Hersteller. Umgesetzt?
	Kennen Sie die Vorteile von Zahlungsverkehrssoftware gegenüber Browser-Banking bzw. der Nutzung von Banking-Apps?	Nein →	Zahlungsverkehrssoftware ermöglicht medienbruchfreiere Informationsflüsse zwischen Zahlungsverkehrs- und Finanzbuchhaltungsprozessen. Nutzen Sie von ihrer Bank empfohlene Zahlungsverkehrssoftware. Umgesetzt?
	Ist das Gerät, mit dem Sie Online-Banking durchführen, frei von Schadsoftware?	Nein →	Führen Sie unter keinen Umständen mit diesem Gerät Online-Banking durch; geben Sie keine sensiblen Daten ein und lassen Sie das System auf dem Gerät neu aufsetzen. Überprüfen Sie zeitnah von einem virenfreien Rechner die Kontoumsätze und ihre offiziellen Kontoauszüge. Umgesetzt?
Anspruch auf Schadenersatz sichern.	Halten Sie die Bedingungen zum Online-Banking der Bank ein und lesen Sie die aktuellen Sicherheitshinweise der Bank?	Nein →	Die Bedingungen zum Online-Banking erhalten Sie bei Vertragsabschluss zum Online-Banking von Ihrer Bank. Aktuelle Sicherheitshinweise sollten Sie auf dem Bankportal verfolgen. Umgesetzt?
	Nutzen Sie ein trojanersicheres Verfahren für die Bestätigung oder Signierung des Auftrags? Beispiele: TAN-Generator mit separater Anzeige und Tastatur, HBCI-Chipkarte mit Secoder 2.	Nein →	Wählen Sie aus den Angeboten Ihrer Bank ein trojanersicheres Verfahren. Vgl. http://www-ti.informatik.uni-tuebingen.de/~borchert/Troja/Online-Banking.shtml Umgesetzt?

Browserbanking

Falls Sie das nicht-trojanersichere smsTAN-Verfahren nutzen: Beachten Sie, dass das Gerät, mit dem die TAN empfangen wurde (z.B. Mobiltelefon), nicht für das Online-Banking genutzt werden darf?

Nein

Umgesetzt?

Die Bestätigung bzw. Signierung des Bankauftrags muss immer über ein sicheres zweites Medium (z.B. Chip-TAN, SmartTAN-plus, HBCI mit Chipkarte und Kartenleser nach Secoder-Standard) erfolgen. Verwenden Sie für den Empfang von smsTan keine internetfähigen Geräte. Vermeiden Sie Telefon-Banking.

Trojaner könnte die Daten manipuliert haben.

Überprüfen Sie die eingegebenen Daten vor ihrer Bestätigung/ Signierung?

Nein

Umgesetzt?

Gleichen Sie die vom TAN-Generator bzw. Secoder dargestellten Daten mit denen des Auftrags ab, bevor Sie diesen bestätigen oder signieren.

Zusätzlich Fragen bei der Nutzung von Browserbanking

Der Bank-Link kann auf eine Phisingseite führen.

Geben Sie die Internetadresse Ihrer Bank unter der Verwendung von https immer manuell in die Browserzeile ein? Prüfen Sie, ob das Schloss-Symbol während der gesamten Verbindungsdauer ungebrochen dargestellt wird und ob das SSL-Zertifikat von Ihrer Bank stammt und gültig ist?

Nein

Umgesetzt?

Kontrollieren Sie, ob die Webseite Ihrer Bank für die Kommunikation *https* statt *http* nutzt; prüfen Sie, ob das Zertifikat auf ihre Bank ausgestellt ist und vergewissern Sie sich im Zweifelsfall bei Ihrer Bank, um die Richtigkeit des Zertifikates zu verifizieren.

Browser stellt Fehlinfor-mationen dar.

Kennen Sie Möglichkeiten, wie man Gefahren durch Man-in-the-Browser-Attacken bzw. browser-injection vermeidet?

Nein

Umgesetzt?

Beim Online-Banking im Browser ist die Verwendung von live-Systemen wie bspw. bankix eine Maßnahmen gegen diese Art von Attacken.

Unberechtigter Zugriff durch Folgenutzer möglich.

Beenden Sie die Bank-Anwendung durch den dafür vorgesehenen Button im Bankportal?

Nein

Umgesetzt?

Verhindern Sie unbefugten Zugriff auf Ihr dann noch geöffnetes Bankportal durch nachfolgende Nutzer.

Erratbare Nutzernamen und PINs erleichtern Hackern den Zugriff.

Haben Sie einen Benutzernamen und ein Passwort bzw. eine PIN nach den Sicherheitsempfehlungen Ihrer Bank gewählt?

Nein

Umgesetzt?

Animieren Sie Mitarbeiter zur Verwendung von ausreichend langen und sinnfrei zusammengesetzten Passwörtern (möglichst mehr als 10 Zeichen) und frei wählbaren Benutzernamen aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Benutzernamen und Passwörter sollten nicht automatisch abgespeichert werden.

Gefahr durch Phishing

Geräte können manipuliert sein.

Ist das Siegel der Authentifizierungsinstrumente (Kartenleser, POS-Zahlungsgerät oder iZettle) verletzt oder ausgetauscht?

Ja →

Umgesetzt?

Notieren Sie sich zur Identifizierung der Siegel deren fortlaufende Seriennummer. Führen Sie unter keinen Umständen Onlinebanking durch; geben Sie keine sensiblen Daten ein. Wenden Sie sich ggf. an den Gerätelieferanten

Verlust vertraulicher Zugangsdaten

Bewahren Sie Ihre Zugangsdaten und das Sicherheitsmedium getrennt voneinander an sicheren Orten auf?

Nein →

Umgesetzt?

Verhindern Sie unbefugten Zugriff auf Ihre Zugangsdaten und Ihr Sicherheitsmedium.

Unkontrollierter Zahlungs-verkehr

Haben Sie ein adäquates Tageslimit für Online-Überweisungen eingerichtet? Und überprüfen Sie regelmäßig Ihre offiziellen Bankauszüge?

Nein →

Umgesetzt?

Lassen Sie sich ein Tageslimit festlegen, welches nur schriftlich und nicht online geändert werden kann. Sollten TAN und PIN doch in die Hände eines Angreifers gelangen, kann im Schadensfall nur eine bestimmte Summe und nicht das gesamte Kontovermögen gestohlen werden.

Phishing und Social Engineering

Kennen Sie Möglichkeiten, wie man Gefahren durch Phishing-E-Mails vermeidet?

Nein →

Umgesetzt?

Ihre Bank würde Sie niemals nach sensiblen Informationen fragen oder im Browser zu Transaktionen auffordern. Teilen Sie niemandem Ihre persönlichen Zugangsdaten mit. Prüfen Sie die Echtheit der Website Ihrer Bank (Zertifikat, https). Nutzen Sie keine TAN-Listen.

Kennen Sie die Gefahren des Social Engineering?

Nein →

Umgesetzt?

Geben Sie unter keinen Umständen sensible Informationen an Personen weiter, die Sie nicht verifiziert haben. Rufen Sie ggf. ihren Bankberater an, um sich rück zu versichern.

Wurde auf weitere Sicherheitstipps zur Steigerung der IT-Sicherheit hingewiesen?

Nein →

IT-Sicherheit im Handwerk
it-sicherheit-handwerk.de

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Task Force „IT-Sicherheit in der Wirtschaft“
Die Task-Force „IT-Sicherheit in der Wirtschaft“ ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern.
Weitere Informationen zur Task-Force und ihren Angeboten sind unter:
www.it-sicherheit-in-der-wirtschaft.de abrufbar
www.it-sicherheit-handwerk.de

itb- Institut für Technik der Betriebsführung im Deutschen Handwerksinstitut e.V.

Heinz-Piest-Institut für Handwerkstechnik an der Leibniz Universität Hannover

Handwerkskammer Rheinhessen, Kompetenzzentrum für IT-Sicherheit und qualifizierte digitale Signatur

if(is)- Institut für Internet-Sicherheit der Westfälischen Hochschule