Merkblatt Informations-Sicherheit für Unternehmen

Dieses Merkblatt soll Unternehmen helfen, ihre Informations-Sicherheit hoch zu halten.

Organisatorische Massnahmen

- Definieren Sie eine Richtlinie (Policy) «Informations-Sicherheit» und lassen Sie diese durch die Geschäftsführung abnehmen.
- Überprüfen Sie regelmässig Ihre Risiken im Bereich Informations-Sicherheit und legen Sie diese der Geschäftsleitung vor.
- Stellen Sie sicher, dass Verantwortlichkeiten bezüglich IT und den damit verarbeiteten Daten geregelt sind. Achten Sie auch darauf, Zuständigkeiten zwischen Ihnen als Anwender und Ihrem IT-Dienstleister klar zu regeln. Schulen Sie Ihre Mitarbeitenden regelmässig im Umgang mit der IT-Infrastruktur hinsichtlich Sicherheit.
- Lassen Sie Ihre IT-Systeme sporadisch von einem externen Spezialisten prüfen.

Technische Massnahmen

Sichern Sie Ihre Daten

Vergewissern Sie sich, dass regelmässige Backups aller relevanten Daten angefertigt werden. Denken Sie dabei auch an die Daten auf Ihrem Smartphone. Vor allem beim Einsatz von cloud-basierten Speichern ist eine vorgängige Verschlüsselung des Backups ratsam. Kontrollieren Sie nach der Sicherung, ob Ihre Daten tatsächlich gespeichert worden sind und auch wieder korrekt zurückgespielt werden können.

Schützen Sie sich gegen digitale Schädlinge

Installieren Sie auf jedem Computer ein Anti-Malware Programm («Virenschutzprogramm») der neusten Generation. Aktualisieren Sie Ihr Anti-Malware Programm, sobald Updates verfügbar sind (meist täglich).

Schützen Sie sich vor Eindringlingen

Überprüfen Sie, ob Sie eine Firewall installiert haben und ob diese aktiviert ist, bevor Sie Ihren Computer mit einem Netzwerk verbinden. Setzen Sie zusätzlich zur auf dem Arbeitsplatz-Computer aktiven Firewall eine dedizierte Firewall bei Internetzugängen ein – allenfalls ist sogar eine Proxy-Infrastruktur angebracht. Eine regelmässige Überprüfung der Firewall-Logs wird empfohlen.

Beugen Sie mittels Software-Updates vor

Aktualisieren Sie Ihre Betriebssysteme (Windows, Mac OS X, Linux, etc.) sowie Ihre Programme regelmässig mit den offiziellen Updates der Hersteller. Denken Sie auch an Ihre Zusatzgeräte wie Smartphones oder die Firmware von Routern, Telefonanlagen, internetfähigen Fernsehgeräten etc.

Software-Portfolio

Laden Sie nur die für Ihr Geschäftsmodell benötigte Software auf Ihre Systeme.

Luzerner Kantonalbank AG, Cash Management Services, Tel. 041 206 24 92, cash@lukb.ch, www.lukb.ch

Stand: 06.02.2017

Verhaltens-Massnahmen

Legen Sie eine gesunde Portion Skepsis an den Tag

- Überlegen Sie gut, wo und wem Sie Ihre persönlichen Daten preisgeben (das gilt auch am Telefon).
- Verhält sich eine Anwendung (insb. Online-Anwendungen wie E-Banking oder Web-Mail) merkwürdig, nehmen Sie Kontakt mit dem entsprechenden Dienstleister oder Hersteller auf.
- Öffnen Sie Anhänge von E-Mails mit Vorsicht – dies gilt leider auch, wenn Ihnen der Absender bekannt ist.
- Wählen Sie sichere Passwörter (siehe «Kriterien für ein sicheres Passwort») und geben Sie die Passwörter niemandem bekannt.
- Wir raten grundsätzlich von der Passwort-Speicherungs-Funktion einiger Anwendungen ab (z.B. Auto-Vervollständigung und Passwort-Speichern im Browser).
- Lesen Sie Warnhinweise und Fehlermeldungen von Anwendungen (online und offline) genau durch und fragen Sie im Zweifelsfall bei einer versierten und vertrauenswürdigen Person nach.
- Lassen sie Ihren gesunden Menschenverstand walten: werden auf der Webseite Ihres Finanzdienstleisters beispielsweise seltsame Meldungen angezeigt (z.B. Wartung ohne Vorankündigung oder Rechtschreibefehler) sollten Sie sicherheitshalber mit dem Dienstleister Kontakt aufnehmen.

Kriterien für ein sicheres Passwort

Grundsätzlich ist es ratsam für Ihre diversen (Online-)Accounts unterschiedliche Passwörter zu verwenden. Falls Sie sehr viele Accounts zu verwalten haben und sich nicht alle Passwörter merken wollen, benutzen Sie am besten einen sog. verschlüsselten Passwort-Safe wie z.B. 1Password oder KeePass (vgl. https://www.ebas.ch/de/5-schritte-fuer-ihre-sicherheit/5-aufpassen). Machen Sie zudem Gebrauch von den «starken Loginverfahren» (sog. 2-Faktoren Authentisierung), wie Sie inzwischen auch von Anbietern wie Google (Gmail, Google Drive), Dropbox oder Microsoft (OneDrive) angeboten werden.

- Benutzen Sie mindestens 8 Zeichen – länger ist besser als kurz und komplex.
- Eine Mischung aus Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen ist ratsam.
- Benutzen Sie keine Tastaturfolgen wie z.B. «asdfg» oder «12345».
- Das Passwort sollte keinen Sinn (z.B. Name, Ort) ergeben.

Erkennen Sie «Phishing»

Phishing ist ein englisches Kunstwort, das sich aus «password» und «fishing» zusammensetzt. Mit gefälschten Webseiten, E-Mails, Kurznachrichten und Telefonaten versuchen Betrüger an persönliche Daten (Benutzererkennung, Passwörter, Konto- und Telefonnummern) zu gelangen. Das Ziel ist es beispielsweise, mit den Daten das Konto eines Opfers zu plündern oder online die Identität des Opfers zu übernehmen (Identitätsdiebstahl).

Phishing beim Verwenden von E-Mail-Diensten

- Verwenden Sie niemals einen Link aus einer E-Mail, um sich beim E-Banking anzumelden. Geben Sie die entsprechende URL manuell, direkt im Browser ein.
- Seien Sie besonders vorsichtig bei E-Mails mit Anhängen – diese Anhänge können Malware (meist einen «Trojaner») enthalten.

Stand: 06.02.2017

- Geben Sie unter keinen Umständen persönliche oder vertrauliche Daten preis. Ein seriöser Dienstleister wird Sie beispielsweise nie nach einem Passwort fragen.
- Löschen Sie E-Mails unbekannter Herkunft im Zweifel sofort, ohne diese vorher zu öffnen.

Phishing beim Surfen im Internet

- Achten Sie darauf, dass Sie stets über eine «sichere» Verbindung («https» und Schloss-Symbol in der Adresszeile vom Browser) mit Ihrem Finanzinstitut verbunden sind. Es darf dabei grundsätzlich zu keinen Warnhinweisen kommen.

Phishing bei Telefongesprächen

- Beenden Sie umgehend Telefongespräche, bei denen Sie nach Passwörter, Kreditkartendaten oder anderen persönlichen Informationen gefragt werden.

Vorgehen wenn Ihre Daten abhandengekommen sind

- Falls Sie bankrelevante Daten wie Passwörter oder Kreditkartendaten einem Betrüger angegeben haben, sollten Sie sich umgehend an den E-Banking Helpdesk wenden (Telefon 0900 844 206 oder info@lukb.ch).
- Wenden Sie sich ebenfalls bei Unsicherheit oder Unklarheiten an uns.

Sicherer Umgang mit Ihrem Smartphone

- Schützen Sie Ihr Smartphone mittels Codesperre vor unbefugten Zugriffen.
- Lassen Sie Ihr Gerät nie unbeaufsichtigt. Gehen Sie mit Ihrem Smartphone gleich sorgfältig um wie mit Ihrem PC.
- Installieren Sie Apps ausschliesslich aus den offiziellen App-Stores der Anbieter (Android → Google Play Store, iOS → Apple App Store).
- Smartphones enthalten standardgemäss relativ hohe Schutzmechanismen. Diese funktionieren aber nur optimal, wenn die Geräte nicht durch den Benutzer modifiziert wurden (kein Jailbreak). Standardmässig verbietet Android die Installation von Apps aus unbekannten Quellen. Diese Einstellung sollte nicht verändert werden (Einstellungen/Sicherheit/«Installation von Apps aus anderen Quellen als dem Play Store zulassen» muss deaktiviert sein).

Weiterführende Informationen zur Sicherheit

Auf der Webseite der Luzerner Kantonalbank finden Sie ausführliche Informationen zur Sicherheit beim Geldbezug am Bancomat, im Internet und im E-Banking.
https://www.lukb.ch/web/lukb/-/sicherheit

Auf der Webseite «eBanking aber sicher» erhalten Sie leicht verständliche und visuell unterstützte Empfehlungen für ein sicherheitsbewusstes Verhalten im E-Banking. Danke, dass Sie mithelfen die Sicherheitskultur im E-Banking zu leben und zu pflegen.
https://www.ebas.ch/de/

Auf der Webseite des Bundes finden Sie wertvolle Informationen zum Schutz vor Gefahren und Risiken im Internet.
https://www.melani.admin.ch/melani/de/home.html

Stand: 06.02.2017