Mit

SICHERHEIT

zu mehr

WOHLBEFINDEN

DATENSICHERHEIT

WORKBOOK + CHECKLISTE

PREPPO GMBH

Workbook

DATENSICHERHEIT

Die Vernetzung mit dem Internet nimmt weltweit immer mehr zu. Täglich verwenden wir Geräte wie Computer, Smartphones und Tablets, die uns die Kommunikation und viele weitere Aufgaben erleichtern. Dabei sind wir oftmals durchgängig rund um die Uhr mit dem Internet verbunden.

Der Zugang zur „digitalen Welt" bringt aber auch viele Gefahren mit sich. Die Berücksichtigung der folgenden Punkte hilft, die Risiken zu minimieren.

1. Sichere Anmeldung bei Online-Diensten
2. Systeme und Software aktuell halten
3. Sichern von wichtigen Daten
4. Die Sache mit dem „Phishing"

Haftungsausschluss: Das vorliegende Dokument kann keine abschließende Gefahrenvorsorge bieten. Es ersetzt keinesfalls ein kontinuierliches und eigenständiges Hinterfragen und Beurteilen von Situationen hinsichtlich Ihres ganz spezifischen Risikopotenzials in Ihrer eigenen häuslichen Umgebung.

© PREPPO GMBH

1. SICHERE ANMELDUNG BEI ONLINE-DIENSTEN

Passwörter

Verwenden Sie, auch wenn dies umständlich erscheint, zum Schutz Ihrer Geräte- und Online-Accounts (z.B. für Ebay und Amazon) jeweils ein eigenständiges Passwort. Dies verhindert, dass bei Bekanntwerden eines Passworts ein Angreifer gleichzeitig überall Zugang erhält. Nehmen Sie bei der Erstellung der Passwörter Abfolgen, die aus möglichst vielen Zeichen –
mindestens acht – bestehen. Die Verwendung von Sonderzeichen steigert deren Sicherheit. Passwörter lassen sich mit Hilfe persönlicher Merksätze einfacher einprägen. Haben Sie besonders viele Passwörter, dann erleichtert eine kostenpflichtige App wie „OnePassword“ deren Verwaltung.

2-Wege Authentifizierung

Als zusätzliche Sicherheitsstufe um Online-Accounts vor Missbrauch durch Dritte zu schützen, empfiehlt es sich die „2-Wege oder auch 2-Faktor Authentifizierung“ zu verwenden. Diese lässt sich in den Sicherheitseinstellungen von Diensten wie z. B. Amazon, Ebay und Paypal aktivieren. Nach erfolgreicher Aktivierung wird bei jedem Anmeldevorgang zusätzlich ein automatisch generiertes Passwort abgefragt, das Sie abhängig von den bereitgestellten Möglichkeiten des Dienstes per Telefonanruf, SMS oder mittels einer zusätzlichen App erhalten.

2. SYSTEME UND SOFTWARE AKTUELL HALTEN

Halten Sie Betriebssysteme und Software sämtlicher mit dem Internet verbundener Geräte, wie PCs, Smartphones, Tablets und Smart-Home Komponenten, stets auf dem aktuellsten Stand, um bestmöglich geschützt zu sein. Nur durch die erfolgreiche Installation aller verfügbaren „Updates“ werden Optimierungen der Gerätehersteller und Softwareunternehmen zur Abwehr akuter Sicherheitsbedrohungen übertragen.

3. SICHERN VON WICHTIGEN DATEN

Sichern Sie persönliche Daten, wie beispielsweise schriftliche Dokumente in Form von Ausarbeitungen am PC oder digitale Bilder vom letzten Familienurlaub, vor dem Verlust. Schon das versehentliche Löschen oder ein technischer Defekt der Festplatte kann dazu führen, dass Sie nur noch unter hohem technischen und damit finanziellen Aufwand wieder an Ihre Daten gelangen können.
Hinzu kommt der jederzeit mögliche Befall des Systems durch Schadsoftware, wie einem Virus oder einem Verschlüsselungstrojaner, der alle Ihre Daten mit sofortiger Wirkung unlesbar macht. Ein gutes Datensicherungskonzept schützt vor Datenverlust. Sie sollten regelmäßig Ihre Daten sichern, wenn möglich zusätzlich an einem externen Ort, um auch im extremen Fall eines Brandes über ein „Backup“ zu verfügen.

© PREPPO GMBH

4. DIE SACHE MIT DEM „PHISHING“

„Aufgrund eines Problems wurde Ihr Konto vorübergehend gesperrt, bitte geben Sie Ihren Benutzernamen und Passwort ein, damit wir Ihr Konto erneut verifizieren können.“
Durch das sogenannte „Phishing“ werden von Kriminellen Passwörter zu Onlinediensten, wie dem Onlinebanking abgefangen (in der Anglersprache heißt das „abgefischt“). Dies geschieht mittels täuschend echt aussehender E-Mail-Nachrichten und Webseiten, verbunden mit der Aufforderung, Ihre Zugangsdaten an- oder einzugeben.

So schützen Sie sich:

Geben Sie niemals Ihre Nutzerkennung und das zugehörige Passwort aufgrund einer an Sie gerichteten Aufforderung an oder ein. Kein seriöses Unternehmen wird Sie jemals zur Bekanntgabe Ihres Passwortes auffordern.

Klicken Sie auch Links in entsprechenden E-Mails nicht an.

Melden Sie dem betroffenen Unternehmen, beispielsweise der Sparkasse, den entsprechenden Betrugsversuch.

© PREPPO GMBH

CHECKLISTE

- [ ] Verwenden Sie für jeden Dienst ein eigenständiges Passwort?
- [ ] Benutzen Sie als Passwort ein Konstrukt aus möglichst vielen Zeichen (mindestens acht) und Sonderzeichen?
- [ ] Enthalten Ihre Passwörter keine Namen von Angehörigen, Geburtstage und dergleichen mehr?
- [ ] Benutzen Sie die 2-Wege-Authentifizierung bei allen Diensten, bei denen sie zur Verfügung steht?
- [ ] Halten Sie die Betriebssysteme und Software stets auf dem aktuellsten Stand?
- [ ] Haben Sie von wichtigen Daten eine Datensicherung angelegt?
- [ ] Ignorieren Sie ganz konsequent Aufforderungen zur Bekanntgabe von Zugangsdaten?

Unsere Empfehlungen

© PREPPO GMBH