STEUERBERATUNG
DIE STEUERFÜCHSE

SICHERHEITS-INFORMATION:

PRÜFE DEIN RECHNUNGSPROGRAMM

DEINE STEUERFÜCHSE AUS KIEL

Wir möchten Dich über einen aktuellen Vorfall informieren, der auch für Deine Sicherheit und die Deiner Daten relevant sein könnte.

Ein langjähriger Kunde eines unserer Mandate hat kürzlich festgestellt, dass die Bankverbindung auf einer Rechnung geändert war. Nach eingehender Prüfung stellte sich heraus, dass sich unbefugte Dritte in das Rechnungsprogramm des Mandanten eingehackt und dort die Stammdaten manipuliert haben – ohne dass der Mandant dies bemerkt hatte.

Um derartige Vorfälle bei Dir zu vermeiden, empfehlen wir dringend, die folgenden Schritte durchzuführen:

1. Hinterlegte Stammdaten prüfen

Überprüfe im regelmäßigen Abstand die in Deinem Rechnungsprogramm hinterlegten Stammdaten wie:

- Bankverbindungen
- Adresse
- Firmenname und Steuernummer

2. Passwort ändern

Ändere das Passwort Deines Rechnungsprogramms jedes Quartal oder halbe Jahr - verwende dabei ein sicheres Passwort:

- Mindestens 12 Zeichen
- Groß- und Kleinbuchstaben
- Zahlen und Sonderzeichen

Falls möglich, aktiviere die Zwei-Faktor-Authentifizierung (2FA) für zusätzliche Sicherheit.

3. Zugriffseinstellungen prüfen

Überprüfe, welche Personen Zugriff auf Dein Rechnungsprogramm haben. Entferne Benutzer, die keinen Zugriff mehr benötigen, und stelle sicher, dass nur autorisierte Personen Administratorrechte besitzen.

Sicherheitsvorfälle wie diese unterstreichen, wie wichtig es ist, auf den Schutz Deiner sensiblen Daten zu achten. Solltest Du Unterstützung bei der Umsetzung dieser Maßnahmen benötigen oder Fragen haben, stehen wir Dir selbstverständlich gerne zur Verfügung.

ZUSATZINFORMATIONEN:
WIE KANN ICH MEINE DATEN IM ALLGEMEINEN SCHÜTZEN

Wie gelangen meine Daten in fremde Hände?

Es gibt mehrere Wege, wie Angreifer an Deine Daten gelangen können:

1. Datenlecks: Wenn Webseiten oder Datenbanken gehackt werden, landen oft Benutzernamen, E-Mails und Passwörter im Internet. Angreifende nutzen diese Daten, um sich auf anderen Seiten mit den gleichen Zugangsdaten anzumelden – oft automatisiert durch Bots.
2. Phishing: Täuschend echte E-Mails fordern Dich auf, Dich auf gefälschten Webseiten anzumelden. Wenn Du Deine Daten dort eingibst, landen sie direkt bei den Angreifenden.
3. Viren und Malware: E-Mails mit schädlichen Anhängen oder Links können Malware auf Deinem Computer installieren. Diese kann Tastaturanschläge aufzeichnen, Passwörter stehlen und Daten über das Internet an die Angreifenden senden.
4. Social Engineering: Angreifende manipulieren Dich, um persönliche Informationen preiszugeben. Sie geben sich als vertrauenswürdige Personen aus (z. B. IT-Support) und nutzen Dein Vertrauen aus.
5. Man-in-the-Middle-Angriffe (MITM): Bei unsicheren Internetverbindungen, wie öffentlichem Wi-Fi, kann eine angreifende Person die Kommunikation zwischen Dir und einer Website abfangen und Deine Daten stehlen.
6. Unachtsamkeit: Einfache Fehler, wie Passwörter auf dem Schreibtisch liegen zu lassen oder auf unsicheren Seiten persönliche Daten einzugeben, machen es Angreifenden leicht.

Wie kannst Du Dich schützen?

1. Starke, einzigartige Passwörter: Verwende für jede Seite ein eigenes Passwort. Nutze lange Passwörter mit einer Mischung aus Zahlen, Buchstaben und Sonderzeichen. Ändere sie regelmäßig.
2. Zwei-Faktor-Authentifizierung (2FA): Aktiviere 2FA, wo immer möglich. Diese zusätzliche Sicherheitsstufe schützt Dein Konto, selbst wenn Dein Passwort gestohlen wird.
3. Überprüfe Datenlecks: Nutze Webseiten wie “Have I Been Pwned”, um zu prüfen, ob Deine E-Mail-Adresse in einem bekannten Datenleck auftaucht. Falls ja, ändere sofort Deine Passwörter.
4. Antiviren-Software und Updates: Halte Dein Betriebssystem und Deine Programme immer auf dem neuesten Stand, um Sicherheitslücken zu schließen. Nutze Antiviren-Software und führe regelmäßig Scans durch.
5. Achtsamkeit bei E-Mails: Sei vorsichtig bei unerwarteten E-Mails, insbesondere wenn sie Dich auffordern, auf Links zu klicken oder persönliche Daten einzugeben. Überprüfe immer die Absenderadresse und den Inhalt auf Unstimmigkeiten.
6. Öffentliche Netzwerke sicher nutzen: Vermeide es, in unsicheren Wi-Fi-Netzen sensible Daten einzugeben. Verwende ein VPN (Virtual Private Network), um Deine Internetverbindung zu verschlüsseln.
7. App-Berechtigungen verwalten: Überprüfe regelmäßig die Berechtigungen von Apps auf Deinem Smartphone oder Computer. Deaktiviere unnötige Zugriffe (z. B. Kamera oder Mikrofon), um Deine Privatsphäre zu schützen.
8. Geräteschutz: Schütze Deine Geräte mit Passwörtern, PINs oder biometrischen Daten (Fingerabdruck, Gesichtserkennung). Bei Diebstahl oder Verlust kannst Du so den Zugriff auf Deine Daten verhindern.