

- Ergebnisse von Unfall- und Berufskrankheiten-Untersuchungen

#### Daten unserer Versicherten im Zusammenhang mit der Teilnahme an Seminarveranstaltungen der Unfallkasse Thüringen

- Stammdaten: Name, Anschrift, Geschlecht, Kommunikationsdaten, Unternehmenszuordnung, Funktions- oder Dienstbezeichnung
- im Falle der Erstattung von Reisekosten: Bankverbindung

#### **Mögliche Risiken und wie Sie sich schützen können**

Es besteht das Risiko, dass Angreifer die gestohlenen Daten für Phishing-Betrügereien, Identitätsdiebstahl oder -betrug und zur Erstellung gefälschter Schreiben oder E-Mails verwenden. Bitte lesen Sie unsere Empfehlungen, wie Sie sich vor diesen Risiken schützen können.

Ein Angreifer, der beispielsweise über Ihre Kontaktdaten verfügt, könnte sich als Vertreter der UKT ausgeben, um Ihnen „Spear-Phishing“-Nachrichten zu senden, die Sie dazu verleiten sollen, dem Angreifer weitere vertrauliche Informationen preiszugeben. Solche Nachrichten könnten sich die Informationen aus Ihren gestohlenen Daten aus der UKT zunutze machen, um sich überzeugender als Vertreter der UKT auszugeben und Ihr Vertrauen zu gewinnen.

Seien Sie vorsichtig bei allen Nachrichten, die Sie erhalten und die scheinbar von der UKT stammen, insbesondere wenn die Nachricht sensible Informationen anfragt oder Sie auffordert, auf Links zu klicken oder Anhänge zu öffnen. Prüfen Sie die Nachricht sorgfältig auf Warnhinweise, die auf Phishing hindeuten, wie beispielsweise eine E-Mail-Adresse, die nicht zur üblichen Schreibweise der E-Mail-Adressen (s.mustermann@ukt.de) passt.

Sollten Sie jemals Zweifel an der Rechtmäßigkeit einer E-Mail, eines Briefes, einer Textnachricht, eines Anrufs oder einer anderen Mitteilung haben, die Sie von der UKT erhalten, setzen Sie sich bitte mit uns in Verbindung.

#### **Welche Maßnahmen haben wir ergriffen?**

Im unmittelbaren Anschluss an den Angriff wurde mit der Forensik und Beweissicherung durch das Landeskriminalamt und einem IT-Dienstleister begonnen. Aus den gewonnenen Erkenntnissen wurden IT-Sicherheitsmaßnahmen abgeleitet und umgesetzt. Die IT-Infrastruktur unterliegt einem permanenten IT Sicherheits-Monitoring.

Wir versichern Ihnen, dass wir bereits im Vorfeld alles Erdenkliche getan haben, um einen Ransomwareangriff auszuschließen. Wir bedauern die Folgen. Dennoch müssen wir feststellen, dass nach den Erkenntnissen und dem Ermittlungsstand erfolgreiche Ransomwareangriffe nicht ausgeschlossen werden können.

#### **Ihr Zugang zum Online-Mitglieder-Service (OMS)**

Das Senden der elektronischen Unfallanzeige wird frühestens ab dem 27.01.2024 wieder möglich sein. Aufgrund des IT- Sicherheitsvorfalls ist es notwendig, dass Ihre Zugangsdaten für den OMS geändert werden. Bei der ersten Abfrage im OMS werden Sie aufgefordert, Ihr Passwort zu ändern. Bitte geben Sie diese Information ggf. an die verantwortlichen Personen weiter.