Haus des Stiftens
Engagiert für Engagierte

FRAGEN UND ANTWORTEN ZU DATENSCHUTZ UND DATENSICHERHEIT

Die folgenden Informationen beziehen sich auf Cyberangriff auf das Haus des Stiftens am 21. September 2024.

WURDEN PERSONENBEZOGENE DATEN ENTWENDET?

Den Angreifern ist es gelungen, trotz umfangreicher technischer Sicherheitsmaßnahmen in großem Umfang Zugriff auf personenbezogene Daten zu erhalten. Wir bedauern dies sehr.

WAS SOLLTE ICH TUN, SOLLTE ICH VON DEM VORFALL BETROFFEN SEIN?

Wir bitten Sie um erhöhte Aufmerksamkeit. Sollten Sie feststellen, dass Ihre Daten missbräuchlich verwendet werden, empfehlen wir, umgehend **Strafanzeige bei der Polizei** zu erstatten und auf diesen Vorfall zu verweisen.
Unter https://www.bsi.bund.de/dok/6700632 finden Sie die amtlichen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für den Umgang mit Identitätsdiebstahl.

Anzeichen für den Missbrauch Ihrer personenbezogenen Daten können vielfältig sein, zum Beispiel:

- Ungewöhnliche Rechnungen oder Mahnungen für Waren oder Dienstleistungen, die Sie nicht bestellt haben.
- Unerklärliche Kontoaktivitäten oder Abbuchungen auf Ihren Bank- oder Kreditkartenkonten.
- Briefe, E-Mails oder Anrufe, in denen Sie aufgefordert werden, zusätzliche persönliche Daten anzugeben oder Zahlungen zu leisten.
- Benachrichtigungen über Anmeldungen oder Änderungen Ihrer Daten bei Diensten, die Sie nicht selbst veranlasst haben.

Überprüfen Sie daher unbedingt regelmäßig Ihre **Bankkonten** und informieren Sie bei auffälligen Transaktionen sofort Ihre Bank und, falls nötig, die Polizei. Überwachen Sie regelmäßig ihr **E-Mail-Konto** und seien Sie vorsichtig bei **ungewöhnlichen Anrufen oder Schreiben**. Löschen Sie **verdächtige E-Mails** unbekannter Absender und **öffnen Sie nicht Links oder Anhänge**. Dies gilt auch für Kommunikation, die vorgibt, von Haus des Stiftens zu stammen.

Ändern Sie vorsorglich alle **Passwörter**, die Sie im Zusammenhang mit dem Haus des Stiftens verwendet haben. Sollten Sie dieselben Zugangsdaten auch bei anderen Diensten genutzt haben, ändern Sie auch dort Ihre Passwörter. Wir empfehlen, für jede Anwendung stets ein einzigartiges, sicheres Passwort zu verwenden.

Tipps für Passwörter finden Sie beim BSI, dem Bundesamt für Sicherheit in der Informationstechnik: Sichere Passwörter erstellen

WELCHE FOLGEN KANN DAS DATENLECK FÜR DEN EINZELNEN HABEN?

Unerwünschte E-Mails: Wenn Ihre Daten in falsche Hände geraten sind, besteht die Wahrscheinlichkeit, dass Sie vermehrt unerwünschte E-Mails erhalten:

- **Spam**, sprich unerwünschte Werbe-Mails.
- **Phishing-Versuche**. Phishing ist eine Betrugsmethode, bei der Kriminelle versuchen, über gefälschte E-Mails, Nachrichten oder Webseiten persönliche Informationen wie Passwörter, Kreditkartendaten oder andere vertrauliche Daten zu stehlen. Sie geben sich oft als vertrauenswürdige Institutionen oder Personen aus und nutzen täuschend echte Kommunikationswege, um das Opfer dazu zu bringen, auf schädliche Links zu klicken oder sensible Daten preiszugeben. Ziel ist es, durch diesen Täuschungsversuch an vertrauliche Informationen zu gelangen oder Geld zu erbeuten.
- Zusätzlich könnte durch Klicks auf Links oder Anhänge von betrügerischen E-Mails **Schadsoftware** auf Ihrem Computer installiert werden. Daher bitte niemals auf Links oder Anhänge von unbekannten Absendern klicken und immer die Absenderadresse prüfen.

Identitätsdiebstahl: Kriminelle könnten Ihre gestohlenen Daten dazu nutzen, um in Ihrem Namen im Internet Einkäufe zu tätigen, Verträge abzuschließen oder Benutzerkonten bei Online-Diensten zu erstellen. Man spricht in diesem Fall von Identitätsdiebstahl. Das kann zu unberechtigten Abbuchungen oder Lastschriften führen – achten Sie deshalb sorgfältig auf Ihre Kontobewegungen.

Sollten Sie Opfer eines Schadens werden, erstatten Sie umgehend persönlich Anzeige bei der Polizei.

KÖNNEN MIT DEN GESTOHLENEN DATEN EINKÄUFE GETÄTIGT ODER VERTRÄGE ABGESCHLOSSEN WERDEN?

Es lässt sich nicht ausschließen, dass mit gestohlenen Daten finanzielle oder rechtliche Handlungen durchgeführt werden können, ohne dass Sie diese autorisiert haben. Das kann beispielsweise bedeuten:

- Unberechtigte Einkäufe oder Bestellungen in Online-Shops
- Das Abschließen von Verträgen (z. B. für Abonnements oder Kredite)
- Überweisungen oder Abbuchungen von Ihrem Bankkonto
- Die Einrichtung von Benutzerkonten bei verschiedenen Diensten, um Leistungen oder Produkte zu erhalten

Aus diesem Grund empfehlen wir Ihnen, Ihre Kontobewegungen aufmerksam zu überwachen.

WIE SOLL ICH MICH VERHALTEN, WENN ICH BEFÜRCHTE, DASS MEINE PERSÖNLICHEN DATEN GESTOHLEN WURDEN?

Seien Sie aufmerksam und skeptisch

Ein vorsichtiges Verhalten ist in Zeiten von Cyberkriminalität immer geraten, nicht nur in diesem Fall. Seien Sie besonders in der nächsten Zeit wachsam bei unerwarteten E-Mails.

Löschen Sie verdächtige E-Mails

Und zwar ohne Anhänge oder Links zu öffnen. Besondere Vorsicht ist geboten, wenn Sie den Absender nicht kennen oder wenn Sie Ihn zu kennen meinen, aber die Mailadresse nicht stimmig scheint.

Vorsicht vor Phishing-Versuchen

Phishing ist eine Betrugsmethode, bei der Kriminelle versuchen, über gefälschte E-Mails, Nachrichten oder Webseiten persönliche Informationen wie Passwörter, Kreditkartendaten oder andere vertrauliche Daten zu stehlen. Sie geben sich oft als vertrauenswürdige Institutionen oder Personen aus und nutzen täuschend echte Kommunikationswege, um das Opfer dazu zu bringen, auf schädliche Links zu klicken oder sensible Daten preiszugeben. Ziel ist es, durch diesen Täuschungsversuch an vertrauliche Informationen zu gelangen oder Geld zu erbeuten. Sogar wenn eine E-Mail von einem unbekannten Absender eine frühere Nachricht von Ihnen zitiert, könnte diese Information aus gestohlenen Daten stammen. Solche Nachrichten sollen Phishing-Versuche glaubwürdiger erscheinen lassen.

Links und Anhänge nicht öffnen

Durch Klicks auf Links oder Mail-Anhänge in betrügerischen E-Mails könnte **Schadsoftware** auf Ihrem Computer installiert werden. Daher bitte niemals auf Links oder Anhänge von unbekannten Absendern klicken und immer ein Auge auf die Absenderadresse werfen.

Anrufe, SMS, WhatsApp

Üben Sie besondere Vorsicht bei Anrufen von unbekannten Nummern. Geben Sie **keine sensiblen Informationen am Telefon** preis. Antworten Sie auch nicht auf **SMS** von unbekannten Absendern. Bei **WhatsApp**-Nachrichten von Unbekannten ist ebenfalls Vorsicht geboten: Löschen Sie solche Anfragen am besten sofort.

Bitte beachten Sie auch die Informationen des Bundesamt für Sicherheit in der Informationstechnik:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-CyberKriminalitaet/Identitaetsdiebstahl/Schutzmassnahmen/schutzmassnahmen_node.html