Apothekerkammer Bremen
Körperschaft des öffentlichen Rechts

Info-Mail der Apothekerkammer Bremen

An alle
Apotheken und Mitglieder
der Apothekerkammer Bremen

Bremen, den 20. Januar 2025

INFO-Mail 2025 Nr. 3

1) Datenschutzvorfall im Antragsportal der D-Trust GmbH

Die D-Trust GmbH ist Ziel eines Angriffs auf das Antragsportal für Signatur- und Siegelkarten geworden. Der Angriff wurde am 13.01.2025 festgestellt. Dabei sind personenbezogene Daten von Antragsstellenden abgerufen und möglicherweise entwendet worden. Nach Aufdecken des Angriffs hat die D-Trust umgehend die Situation ausgewertet und Sofortmaßnahmen ergriffen, um den Schutz der Daten im Portal sicherzustellen. Es wurde Strafanzeige gegen Unbekannt gestellt. Ein spezialisiertes IT-Sicherheitsteam der D-Trust arbeitet eng mit den zuständigen Behörden zusammen, um die Hintergründe des Angriffs aufzuklären. Ob auch Daten Bremer Mitglieder entwendet wurden, ist uns nicht bekannt.

Wir haben heute als Kartenherausgeber die Landesdatenschutzbehörde informiert.

Hierzu einige weitere Details:

1. Welche Ausweisdaten sind genau betroffen?

   Möglicherweise betroffen sind die unten beschriebenen Daten (siehe Tabelle). Personenbezogene Daten aus den D-Trust vorliegenden Identifizierungen enthalten nie eine CAN und auch keine auf den Ausweisen vorhandenen biometrischen Daten (z. B. Foto, Größe, Augenfarbe). Daten der Identifizierung beziehen sich immer auf Namen, Geburtsdaten und/oder Meldeadressen. Es sind keine Kopien von Ausweisen oder Bilddateien/Fotos entwendet worden.

2. Ist eine Sperrung der möglicherweise betroffenen Ausweisdokumente notwendig?

   Eine Sperrung Ihres Ausweisdokuments ist nicht erforderlich. Die möglicherweise entwendeten Daten können nicht zur Nutzung der Online-Ausweisfunktionen genutzt werden. Eine Identifizierung anhand der Daten kann ohne Vorliegen des physischen Ausweises nicht erfolgen. Daher ist ein neuer Ausweis nicht erforderlich, kann aber in bestimmten Fällen angeraten sein. Bitte informieren Sie sich auf der Seite des BSI, die beratende Informationen bereithält.

3. Ist eine präventive Information an Finanzinstitute etc. ratsam?

   Bei Datendiebstahl empfiehlt sich eine Meldung bei der Polizei vorzunehmen spätestens, wenn Sie die betrügerische Verwendung ihrer Daten feststellen. Als Privatperson können betroffene Nutzende eine Anzeige erstatten. Bitte informieren Sie sich auch auf der Seite des BSI zum Thema Identitätsdiebstahl. D-Trust selbst hat unverzüglich eine Anzeige beim

Landeskriminalamt Berlin erstattet.

4. Ist eine Änderung der Login-Daten (E-Mail oder Passwort) für das D-Trust Portal erforderlich? (Diese Frage bezieht sich ausschließlich auf das D-Trust Portal, nicht auf das eHealth-Antragsportal.)

   Nein. Die Logins sind nicht von der Entwendung der Daten betroffen. Es besteht jederzeit für Sie die Möglichkeit, über die Passwort-Vergessen-Funktionalität ein neues Passwort für Ihren Zugang zu generieren. Zusätzlich finden Sie nach Login im Portal unter den Eigenschaften die Möglichkeit, einen zweiten Faktor für den Login zu hinterlegen.

5. Müssen Zertifikatsprodukte gesperrt werden, nachdem hier Daten entwendet wurden?

   Nein. Eine Sperrung Ihres Zertifikatsprodukts ist nicht erforderlich. Bei der Entwendung der Daten wurden keine Zertifikatsprodukte kompromittiert. Ein Antrag auf ein neues Zertifikatsprodukt ist immer mit Ihrer persönlichen Identifikation verbunden. Änderungen (z.B. bei Angabe einer abweichenden Lieferadresse) erfordern immer eine erneute Identifizierung. Diese kann nicht nur auf Basis von Daten erfolgen, sondern bedingt immer den physischen Besitz ihres Ausweisdokuments.

6. Wie schützen Sie sich als Organisation vor Phishing-Attacken?

   D-Trust rät grundsätzlich dazu bei Anfragen per E-Mail oder Telefon vorsichtig zu agieren. Täter versuchen dabei an persönliche Informationen zu gelangen. Die D-Trust wird Sie nie direkt kontaktieren, um Passwörter zu erfragen oder Passwortwechsel oder Re-Identifizierungen anzusprechen. Bitte seien Sie in den kommenden Monaten besonders wachsam bzw. sensibilisieren Sie ggf. ihre Nutzenden entsprechend. In Zweifels- oder Verdachtsfällen wenden Sie sich bitte immer direkt an Ihren Ansprechpartner bei der D-Trust oder an kontakt@d-trust.net.

7. Wie können betroffene Personen sich gegen Identitätsdiebstahl schützen?

   a. Bitte beachten Sie, dass das Thema Identitätsdiebstahl viele Facetten haben kann. Im Zusammenhang mit dem Thema Phishing sollten Sie immer aufmerksam sein, wenn Sie Anfragen per E-Mail oder Telefon erhalten. Die D-Trust GmbH wird Sie nie direkt kontaktieren, um Passwörter zu erfragen oder Passwortwechsel oder Re-Identifizierungen anzusprechen. Bitte seien Sie in den kommenden Monaten besonders wachsam bzw. sensibilisieren Sie ihre Nutzer entsprechend. In Zweifels- oder Verdachtsfällen wenden Sie sich bitte immer direkt an Ihren Ansprechpartner bei der D-Trust oder an kontakt@d-trust.net.

   b. Informationen zum Thema finden Sie unter anderem auf der Internetseite des Bundesamts für Sicherheit in der Informationstechnik (Webseite des BSI unter „Methoden der Cyber-Kriminalität“).

Zeitpunkt des Vorfalls

Der Angriff fand im Zeitraum vom 01.01.25 bis 06.01.2025 statt. Seit dem 06.01.2025 sind keine Zugriffe mehr erfolgt. Der Angriff wurde am 13.01.2025 entdeckt und es wurden umgehend Maßnahmen eingeleitet, so dass keine weiteren Zugriffe erfolgen können.

Betroffene Datenarten

Datenkategorie	SMC-B	eHBA
projectArticleNumber	x	x
Title, Vorname, Nachname	x	x
Geburtsdatum	x	x
Ident-Dokument Nr	teilweise	teilweise
Geburtsort	x	x
Gültigkeitsdatum des Ausweises	teilweise	teilweise
Tag der Ausstellung	teilweise	teilweise
Ausstellende Behörde	teilweise	teilweise
Adresse	x (Praxisadresse)	x (Meldeadresse)
Telefon	x	x
Kontakt e-Mail Adresse	optionales Feld	optionales Feld
Beruf	-	x
Akademische Grade		optionales Feld
Lieferadresse	x	x
Rechnungsadresse	x	x
Bestellnummer	optionales Feld	optionales Feld
Kundennummer	optionales Feld	optionales Feld
Druckzeile1	-	x
Druckzeile2	-	x
Organisationsname	x	-
Organisationsadresse	x (Praxis Adresse)	x (Praxis Adresse)
Gesellschaftsform inkl. Handelsregister Nr.	x (Praxis Name, kein Handelsregister)	x (Praxis Name, kein Handelsregister)

Welche Gegenmaßnahmen wurden eingeleitet/sind geplant?

- Sofortmaßnahmen, Gegenmaßnahmen
  - » Benutzeraccount des Angreifers wurde gesperrt
  - » Abschaltung des D-Trust Portals
  - » Weiterführung der Vorfallanalyse und Bildung eines Incident Response Teams
  - » Entwicklung, Test und Aktivierung Hotfix zur Behebung der Schwachstelle
  - » Daten- und Ausmaßanalyse
  - » Automatische Überprüfung aller Neu-Anmeldungen
  - » Speicherung der verfügbaren Logs zur Beweissicherung
- Weitere Maßnahmen
  - » Relevante Aufsichtsstellen und Konformitätsbewertungsstellen wurden informiert.
  - » Zusätzlich zum internen SOC-Team wurde der Partner von D-Trust im Bereich IT-Forensik beauftragt den Vorfall zu analysieren und einen weiterführenden Plan für zusätzliche Schutzmaßnahmen unter Einbeziehung der Strafverfolgungsbehörden zu

erarbeiten Die Zusammenarbeit wurde zeitnah initiiert und am 15. Januar aufgenommen.

» Die betroffenen VM-Systeme sind gesichert und werden neben den Log-Daten dem Dienstleister zur Analyse zur Verfügung gestellt
» Es wurde durch die D-Trust Strafanzeige gegen Unbekannt gestellt.

Bitte wenden Sie sich bei allen Anfragen zum Vorfall an kontakt@d-trust.net.

2) BeratungsCheck der Kammer Bremen mit neuem Schwerpunkt

Die Kammer Bremen hat auch in diesem Jahr wieder die Avoxa – Mediengruppe Deutscher Apotheker GmbH beauftragt, BeratungsChecks in 25 Apotheken in Bremen durchzuführen. Die Beratungsgespräche werden in diesem Jahr bundesweit zu dem Schwerpunktthema „Erkältungsbeschwerden“ stattfinden. Zu den üblichen Erkältungssymptome zählen zum Beispiel Husten, Schnupfen, Halsschmerzen und Fieber.

Die BeratungsChecks sind eine externe Maßnahme zur Qualitätssicherung: Das Beratungsgespräch wird hinsichtlich seiner Stärken und Verbesserungspotentiale ausgewertet. Der Bewertung liegen die Leitlinien der Bundesapothekerkammer zur Information und Beratung bei der Abgabe von Arzneimitteln zugrunde. Im Feedbackgespräch zwischen beratender Person, Apothekenleitung und Pseudo Customer werden gemeinsam Maßnahmen zur weiteren Qualitätsoptimierung erarbeitet. Somit ist das Konzept darauf ausgelegt, die Apotheken im Erreichen der Beratungsziele zu unterstützen. Es steht hier ein edukativer Ansatz im Vordergrund, nicht die Kontrolle. Die BeratunsgCheck sollen dazu dienen, die Qualität der Beratung in der Selbstmedikation nicht aus den Augen zu verlieren.

Die Information und Beratung zur Abgabe von Arzneimitteln in den öffentlichen Apotheken ist eine pharmazeutische Tätigkeit. Bei der Abgabe von Arzneimitteln an einen Patienten oder eine Patientin ist durch Nachfrage festzustellen, inwieweit dieser oder diese Informations- und Beratungsbedarf hat. um eine den Anforderungen nach § 20 Apothekenbetriebsordnung entsprechende Beratung anzubieten.

Die Verfahrensweise zur Information und Beratung werden mit den Leitlininen der Bundesapothekerkammer "Information und Beratung des Patienten bei der Abgabe von Arzneimitteln - Selbstmedikation" beschrieben. Die Leitlinien der Bundesapothekerkammer finden Sie unter https://www.abda.de/fuer-apotheker/qualitaetssicherung/leitlinien/leitlinien-und-arbeitshilfen/information-und-beratung/#c5726

Auch ist es für Apotheken möglich, selbst einen Pseudo Customer-Besuch zu buchen: https://pseudo-customer.net/online-anmeldung/

Weitere Informationen finden Sie auch unter: https://www.abda.de/fuer-apotheker/qualitaetssicherung/angebote-qs-kammern/pseudo-customer/

3) „Digital Public Health“ – Podcast des BIPS mit Dr. Stefan Schwenzer

Vorstandsmitglied Dr. Stefan Schwenzer hat an der Erstellung eines Podcasts mitgewirkt, der am Leipniz-Institut für Präventionsforschung und Epidemiologie (BIPS) zum Thema „Digital Public Health“- Digitalisierung der Arzneimittelversorgung produziert wurde.

In der Podcast-Reihe „Digital Public Health,“ wird mit unterschiedlichsten Personen über die Möglichkeiten und Auswirkungen der Digitalisierung im Bereich Gesundheit gesprochen. Dabei geht es sowohl um die Chancen, aber auch um kritische Diskussionen der Herausforderungen und Gefahren der Digitalisierung. Das BIPS wollte die Sicht der Apotheken insbesondere zum Thema Digitalisierung der Arzneimittelversorgung aufgreifen.

Unter folgenden Links kann sie angeschaut bzw. angehört werden:

YouTube: https://www.youtube.com/watch?v=ibKtEisZmHU
Spotify: https://open.spotify.com/show/3SsCywm0UbPld219V2u7XW
Apple: https://podcasts.apple.com/us/podcast/digital-public-health-podcast/id1740066840
Deezer: https://www.deezer.com/de/show/1000833701
Webseite BIPS: https://www.digital-public-health.de/podcast.html

Die Dauer beträgt ca. 30 Minuten und spiegelt den Alltag der Apotheken in diesem Bereich wider.

Erste Rezension einer Kollegin: *„Ein spannender Podcast, der zeigt, wie wichtig die digitale Transformation für Apotheken ist! FRAG DIE APOTHEKE setzt bereits heute auf digitale Beratung, um Apotheken als Gesundheitsmanager zu stärken. Mit unserem 24/7-Service bieten wir schnelle, zuverlässige Unterstützung – auch bei Medikationsfragen und Prävention. Wir freuen uns, Teil des digitalen Wandels im Gesundheitswesen zu sein!“*

Mit freundlichen Grüßen,

APOTHEKERKAMMER BREMEN

Dr. Isabel Justus