2025-01-17 Datenschutzvorfall D-TRUST/Bdr

Update seitens D-TRUST zum Datenschutzvorfall

Sehr geehrte Damen und Herren,

Sie erhalten diese E-Mail, da Sie als Herausgeber eines D-Trust-Produktes agieren. Als verantwortliche Stelle sind Sie gemäß Artikel 33 DSGVO zur Meldung des Vorfalls bei der zuständigen Datenschutzaufsichtsbehörde verpflichtet.
Da die D-Trust auch Daten in Eigenverantwortung verarbeitet, haben wir den Vorfall am 16.01.2025 an die Berliner Beauftragte für Datenschutz gemeldet. Ein Aktenzeichen liegt derzeit noch nicht vor und wird Ihnen unaufgefordert mitgeteilt. Es wurde außerdem beim Landeskriminalamt Berlin Strafanzeige gegen Unbekannt erstattet.
Für Ihre Meldung/Unterlagen fügen wir eine Beschreibung der Art der Verletzung bei (siehe unten).
Uns erreichten bereits mehrere Rückfragen, mit Bitte um Empfehlungen zum weiteren Vorgehen. Hierzu haben wir Folgendes zusammengestellt:

1. Welche Ausweisdaten sind genau betroffen?
    a. 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?
    a. 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?
    a. 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.)
    a. 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?
    a. 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?
    a. 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 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.

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“).

Im Folgenden möchten wir Sie über den Hergang des Vorfalls sowie die Details informieren:

<u>Beschreibung des Vorfalls</u>

- 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.
  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 unser Partner 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.

Wir halten Sie weiterhin auf dem Laufenden.

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

Mit freundlichen Grüßen
Michael Sluyter

D-Trust PSM – Senior Service Manager Projects & Operations

D-TRUST GmbH
Kommandantenstr. 15
10969 Berlin

T + 49 (0) 30 – 2598 - 3853
M +49 (0) 151 - 117 72 752

m.sluyter@d-trust.net
www.d-trust.net
michael.sluyter@bdr.de

Aktuelle Einschätzung

In Kürze:

1. Der Kartenherausgeber (die Kammer) ist Verantwortlicher im Sinne von Artikel 4 Nummer 7 DSGVO.
2. wir empfehlen eine zeitnahe Information des Landesdatenschutzbeauftragten (LFDI) durch die Kammer
3. anhand der betroffenen Daten und des damit verbundenen Risikos KÖNNTE man erwägen, die betroffenen Ärzte nicht direkt zu informieren (sondern bspw. nur über die Webseite der Kammer)
4. auf Grund der politischen Ebene (ePA-fürAlle Einführung und -Hack des CCC sowie auch SMC-B betroffen) empfehlen wir die direkte Information der Betroffenen (per Mail, nächste Woche)
    a. die D-TRUST haben wir aufgefordert (s.u.) die konkreten Namen der Betroffenen den jeweiligen Kammern zu benennen

Anschreiben der D-TRUST an die Kammern (Bsp.!)

Von: Datenschutz <datenschutz@d-trust.net>

am: Do 16.01.2025 gegen 19:00

###

Sehr geehrte Damen und Herren,

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 auch möglicherweise personenbezogene Daten von "*ZAHL der BETROFFENEN (siehe Tab.)*" Antragstellern entwendet worden. Da in diesem Zusammenhang mit Ihrer Organisation eine Auftragsverarbeitung der Daten stattfindet, weisen wir Sie darauf hin, dass Ihre Kunden in diesem Zusammenhang zu informieren sind. Teilen Sie uns bitte mit wie wir Sie unterstützen können. 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. Nach bisherigem Stand der Auswertung handelt es sich bei den personenbezogenen Daten um Vor- und Nachname, E-Mail-Adresse, Geburtsdatum, ggfls. Adressdaten sowie ggfls. Nummer des Ausweisdokuments. Es wurden keine Zugänge (Login, Passwortdaten) oder auch Zahlungsinformationen abgerufen. Die Funktion und Sicherheit der ausgegebenen eHBA und SMC-B sind nicht beeinträchtigt. Die Karten können weiter wie gewohnt genutzt werden. Wir gehen derzeit davon aus, dass der Vorfall gezielt auf eine Störung des Geschäftsbetriebs der D-Trust GmbH ausgerichtet war. Gleichwohl ist nicht auszuschließen, dass die möglicherweise entwendeten Daten auch zu Betrugsversuchen genutzt werden.

Als Datenschutzbeauftrage der D-Trust ist Frau Uta Roßberg bestellt. Bitte richten Sie Ihre weiteren Rückfragen an die E-Mail-Adresse datenschutz@d-trust.net.

Wir bedauern die daraus entstehenden Umstände und bitten um Ihr Verständnis.

Mit freundlichen Grüßen

Toni Habich

D-Trust GmbH | Ein Unternehmen der Bundesdruckerei
Kommandantenstr. 15
10969 Berlin

T + 49 (0) 30 – 2593 91 – 0
F + 49 (0) 30 – 2593 91 – 22
datenschutz@d-trust.net
www.d-trust.net
###

Information auf der Webseite der D-TRUST

https://www.d-trust.net/de/newsroom/news/information-datenschutzvorfall-13-januar-2025

Presseecho

https://www.heise.de/news/Vertrauensdiensteanbieter-D-Trust-informiert-ueber-Datenschutzvorfall-10246338.html

Übersicht der betroffenen Kammern

	Nachricht von D-Trust erhalten?	Anzahl der Betroffenen	Anmerkungen

Baden-Württemberg	ja		
Nordwürttemberg	ja		
Südwürttemberg	ja		
Nordbaden	ja		
Südbaden	ja		
Bayern	ja	2144	
Berlin	ja	824	
Brandenburg	ja	287	
Bremen	ja	103	
Hamburg	ja (aber keine Aussage zu Betroffenen!)		
Hessen	ja	720	
Meckl.-Vorpommern	ja	208	
Niedersachsen	ja	1348	
Nordrhein	ja	1998	
Rheinland-Pfalz	ja		
Koblenz	ja	144	
Rheinhessen	ja	99	
Pfalz	ja		
Trier	ja	42	
Saarland			
Sachsen-Anhalt	ja		
Sachsen	ja	83	
Schleswig-Holstein	ja	378	
Thüringen	ja	390	
Westfalen-Lippe	ja	1638	
SUMME		10.315	

Unsere Fragen an D-TRUST zur Aufklärung

Wir hätten gern von D-TRUST gewusst:

- genauere Details zum Datenschutzvorfall und die Gegenmaßnahmen der D-TRUST
  - nach unserem Verständnis sind im Antragsportal nicht sämtliche Vorgänge, sondern nur aktuelle erreichbar, oder?
- wir hätten gern auch von D-TRUST eine Übersicht, welche Kammern mit welcher quantitativen Anzahl an Betroffenen betroffen sind
- wenn eine Information des BfDI durch die D-TRUST erfolgte, hätten wir gern diese Information zK
  - wenn keine Information des BfDI durch die D-TRUST erfolgte, hätten wir gern die Argumentation/Einschätzung, warum dies nicht notwendig ist
- wir wüssten auch gern, warum die Information erst gestern erfolgte (der Vorfall aber bereits am 13.01. entdeckt (?) wurde)

1. alle betroffenen Kammern benötigen für eine etwaige Information der betroffenen Ärzte die genaue Benennung dieser
   a. aktuell noch in Klärung, ob direkte Information der Betroffenen notwendig
   b. besteht nach Ihrer Einschätzung die Pflicht gem. Art. 34 DSGVO die Betroffenen zu benachrichtigen?
2. auf ihrer Webseite (https://www.d-trust.net/de/newsroom/news/information-datenschutzvorfall-13-januar-2025) steht, dass der Vorfall bereits am 13.01. stattfand. Eine Information erfolgte erst am 16ten.
   a. Wann genau wurde der Vorfall bei Ihnen entdeckt? Vllt. sollte Ihre Veröffentlicht diebzgl. sprachlich angepasst werden?
   b. D.h. wir benötigen den Zeitpunkt des Vorfalls und den Zeitpunkt der Kenntnisnahme.
3. Wurde positiv festgestellt, dass eine Verletzung des Schutzes personenbezogener Daten stattgefunden hat ODER wird dies gegenwärtig nur vermutet und noch geprüft ODER kann eine Verletzung des Schutzes personenbezogener Daten aus technischen Gründen nicht positiv festgestellt werden, so dass sie angenommen werden muss?
4. wir benötigen eine genaue Beschreibung der Datenpanne.
5. Welche Datenarten sind genau betroffen. Weitere als die bislang Genannten?
6. Welche Folgen der Verletzung des Schutzes personenbezogener Daten halten Sie für wahrscheinlich?
7. Welche Gegenmaßnahmen haben Sie bereits eingeleitet, welche weiteren Gegenmaßnahmen sind geplant? Inwiefern ist der Herausgabeprozess weiterhin von dem Angriff betroffen?

Schreiben an die GFs der Kammern

(gesendet: 17.01.2025 14:24)

Sehr geehrte Damen und Herren,

wir wurden darüber informiert, dass die D-TRUST GmbH, ein Auftragnehmer der Ärztekammern, Ziel eines Angriffs auf das Antragsportal für u.a. elektronische Heilberufsausweise geworden ist. Der Angriff wurde am 13. Januar 2025 festgestellt. Nach Angaben der D-TRUST könnten dabei personenbezogene Daten wie Vor- und Nachname, E-Mail-Adresse, Geburtsdatum, ggfs. Adressdaten sowie ggfs. Nummern von Ausweisdokumenten kompromittiert worden sein. Die Funktionalität und Sicherheit der ausgegebenen eHBA und SMC-B Karten ist laut D-TRUST nicht beeinträchtigt. Zwei Kammern haben die Information der D-TRUST bislang nicht erhalten. In einer ersten groben Schätzung gehen wir von Daten von akt. mind. 7.000 betroffenen Ärzten aus.

Das Telematik-Dezernat der Bundesärztekammer sendete uns folgende Aufstellung von Empfehlungen und Maßnahmen:

- Die betroffenen Kammern sollten den jeweiligen Landesdatenschutzbeauftragten zeitnah informieren.
    - Der Kartenherausgeber (die Kammer) ist Verantwortlicher im Sinne von Artikel 4 Nummer 7 DSGVO gem. dem mit D-TRUST abgeschlossenem AVV.
- Eine direkte Benachrichtigung der betroffenen Kammermitglieder wird auf Grund der politischen Dimension aktuell empfohlen (bspw. per Mail).
    - D-TRUST wurde gebeten, die betroffenen Personen den jeweiligen Kammern namentlich zu benennen, um eine zielgerichtete Information zu ermöglichen.
    - Alternativ könnte eine Information über die Webseite der Kammern erwogen werden. Die Kammern sollten aber einheitlich handeln und die pol. Dimension berücksichtigen. (ePA-für-Alle)
- Die BÄK befindet sich in enger Abstimmung mit der D-TRUST und weiteren relevanten Stellen (gematik), um den Vorfall aufzuklären und weitere Maßnahmen zu koordinieren.
- Es wurde eine Sitzung der Task-Force Sicherheit bei der gematik einberufen. Weitere Sektoren, bspw. die KVen für die SMC-B sind ebenso betroffen.
    - Die Task Force tagt heute.

Für die Mitglieder der Arbeitsgruppe eArztausweis ist eine Wiki-Seite eingerichtet, wo sämtliche Informationen zusammengeführt werden (siehe auch Anhang):
https://wiki.baek.de/dokumente/pages/viewpage.action?pageId=253067488

Für Rückfragen und weitere Abstimmungen steht Ihnen das Dezernat 5 der Bundesärztekammer (dezernat5@baek.de) selbstverständlich zur Verfügung.

Entwurf eines Schreibens zur Information der Betroffenen

(*noch unabgestimmt)*

Betreff: Wichtige Information zum Datenschutzvorfall bei D-TRUST

Sehr geehrte(r) Herr/Frau *[Vorname und Name des Betroffenen]*,

wir möchten Sie darüber informieren, dass die D-TRUST GmbH, ein Dienstleister der *[Name Ihrer Kammer]*, Ziel eines Angriffs auf das Antragsportal für u.a. elektronische Heilberufsausweise geworden ist. Der Angriff wurde am 13. Januar 2025 festgestellt. Nach bisherigen Erkenntnissen könnten dabei Ihre folgenden personenbezogenen Daten betroffen sein:

- Vor- und Nachname
- E-Mail-Adresse
- Geburtsdatum
- Ggfs. Adressdaten
- Ggfs. Nummer des Ausweisdokuments

Datenkategorie	eHBA
projectArticleNumber	x
Title, Vorname, Nachname	x
Geburtsdatum	x
Ident-Dokument Nr	teilweise
Geburtsort	x
Gültigkeitsdatum des Ausweises	teilweise
Tag der Ausstellung	teilweise
Ausstellende Behörde	teilweise
Adresse	x (Meldeadresse)
Telefon	x
Kontakt e-Mail Adresse	optionales Feld
Beruf	x
Akademische Grade	optionales Feld
Lieferadresse	x

Rechnungsadresse	x
Bestellnummer	optionales Feld
Kundennummer	optionales Feld
Druckzeile1	x
Druckzeile2	x
Organisationsadresse	x (Praxis Adresse)
Gesellschaftsform inkl. Handelsregister Nr.	x (Praxis Name, kein Handelsregister)

Was bedeutet das für Sie?
Nach den uns vorliegenden Informationen sind keine sensiblen Zugangsdaten (wie Passwörter) oder Zahlungsinformationen betroffen. Auch die Funktion und Sicherheit der ausgegebenen elektronischen Heilberufsausweise (eHBA) und Praxisausweise (SMC-B) sind nicht beeinträchtigt. Diese können weiterhin wie gewohnt genutzt werden.

Welche Maßnahmen wurden ergriffen?
Die D-TRUST GmbH hat sofort nach Feststellung des Angriffs Maßnahmen eingeleitet, um die Sicherheitslücke zu schließen. Weitere Informationen finden Sie auf der Webseite der D-TRUST unter: https://www.d-trust.net/de/newsroom/news/information-datenschutzvorfall-13-januar-2025

Unsere Empfehlung an Sie:
Bitte seien Sie besonders aufmerksam bei unerwarteten E-Mails oder Anrufen, in denen persönliche Informationen abgefragt werden. Sollten Sie verdächtige Aktivitäten feststellen, informieren Sie uns bitte umgehend.

Kontakt und weitere Informationen:
Für Rückfragen oder weitere Informationen steht Ihnen Ihre *[Name Ihrer Kammer]* unter *[Kontaktinformationen]* zur Verfügung. Alternativ können Sie sich auch direkt an die D-TRUST GmbH wenden (E-Mail: datenschutz@d-trust.net).

Wir bedauern die entstandenen Unannehmlichkeiten und danken Ihnen für Ihr Verständnis.

Mit freundlichen Grüßen
[Name des Verantwortlichen]
[Position]
[Kontaktinformationen]

Task-Force-Sicherheit der gematik

Die gematik hat in der heutigen Sitzung der TF Sicherheit folg. "reaktive Sprachregelung" (17.1.2024, 14 Uhr) formliert und wird damit ggü. der Presse wie folgt informieren:

"*Wie die D-Trust GmbH mitteilt, hat das Unternehmen am 13.01.2025 einen Datenschutzvorfall in ihrem Antragsportal für Signatur- und Siegelkarten festgestellt. Nach unserer Kenntnis betrifft der Datenschutzvorfall nicht die Telematikinfrastruktur (TI).*
Wir bitten Sie, sich bei weiteren Fragen an die Kommunikation der D-Trust zu wenden."

Ansonsten bleibt aus der Sitzung zu erwähnen, dass

- die anderen LEO weitestgehend verschont worden sind und nur in homöopathischen Dosen betroffen sind (bspw. 3 SMC-B der Krankenhäuser)
- insgesamt sind aber lt. D-TRUST 34.000 Datensätze betroffen
  - wir nehmen an, die Differenz aus 34.000 und den in unserem Sektor Betroffenen sich aus normalen Signaturkarten ergibt (*noch in Klärung!*)
- das DB-Backend wurde über das Webfrontend eines anderen Sektors angegriffen
- die Lücke ist mittlerweile gefixt und die Antragsportale sind online
- sowohl BNetzA als auch Berliner DSB ist informiert worden
  - wir haben erneut die Information erbeten
- Heise hat bereits "Witterung" aufgenommen

Leitlinie der Datenschützer zur Meldung von Vorfällen (ab Seite 29)

Backlog

1. Prüfen, ob die Ausweisnummer (des nPA oder des eHBA) seitens der Kammern in irgendeiner Art und Weise in Zshg. mit Authentifizierungen genutzt wird!
2. Siegelkarten betrachten wir hier nicht, weil diese von DTR/BDr verantwortet werden. Aber deren Nutzer (in ÄKB und ÄKHH) wurden auch angeschrieben.