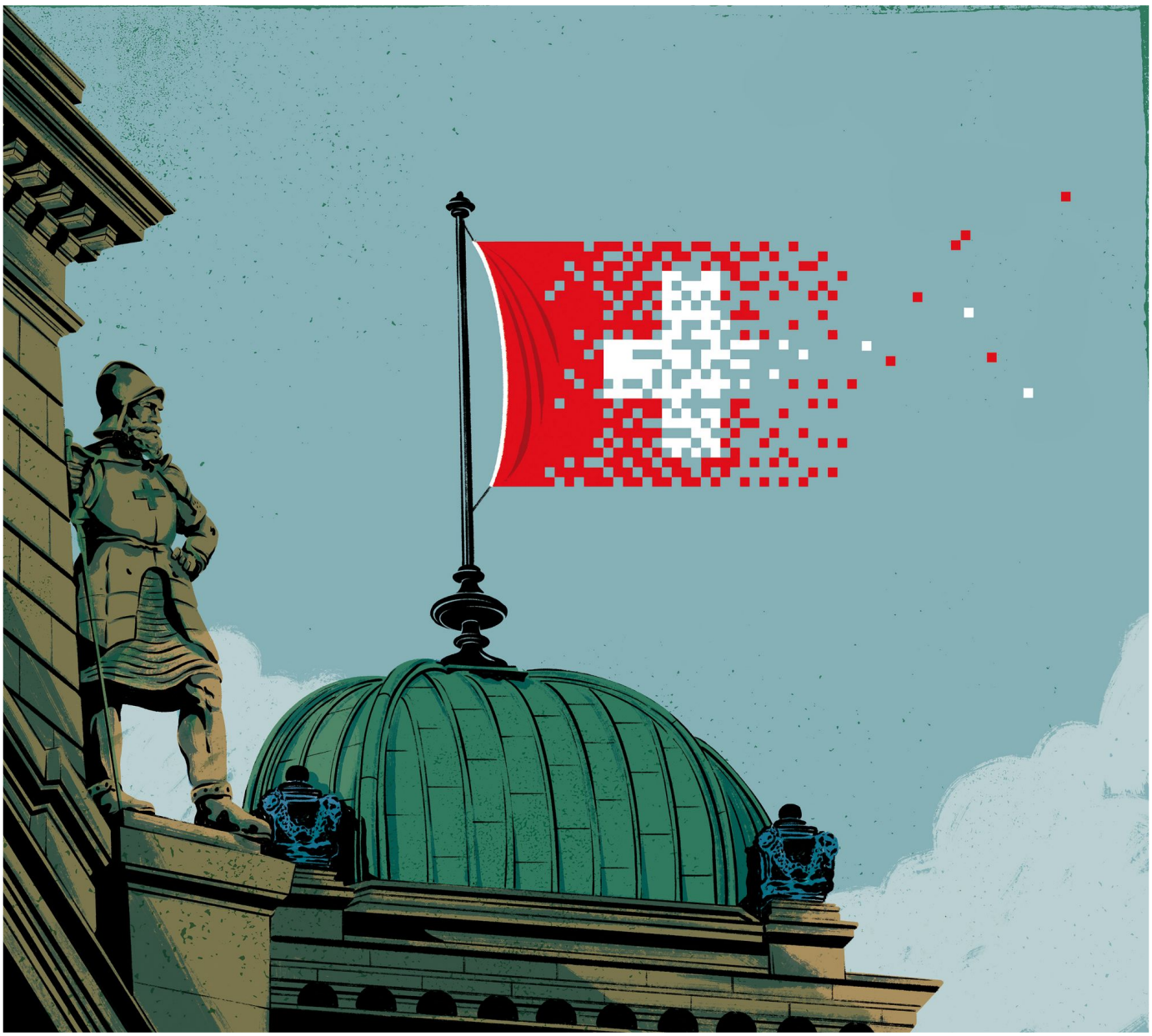

Xplain – ein Beschaffungsskandal

Die gehackte Firma Xplain war «too big to fail»: wie das Unternehmen aus Interlaken zum unverzichtbaren Monopolisten für die Behörden wurde. Und wie diese es versäumten, Auflagen zur IT-Sicherheit zu machen.

Von Adrienne Fichter (Text) und Adrià Fruitós (Illustration), 25.09.2023

Die Telefondrähte laufen heiss, Bundesangestellte arbeiten bis zur Erschöpfung, Sitzungen werden hastig einberufen, Medienanfragen geblockt, auf das Öffentlichkeitsgesetz gestützte Einsichtsgesuche auf den

Sankt-Nimmerleins-Tag aufgeschoben. Seit Wochen herrscht hektisches Treiben

- bei der Beschaffungsstelle des Bundes, dem Bundesamt für Bauten und Logistik;
- beim Bundesamt für Polizei, beim Fedpol;
- beim Bundesamt für Zoll und Grenzsicherheit (BAZG);
- beim Bundesamt für Rüstung, bei der Armasuisse;
- beim Bundesamt für Justiz;
- beim Nachrichtendienst des Bundes;
- beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten
- und nicht zuletzt beim Nationalen Zentrum für Cybersicherheit.

Der Grund: der massive Datenabfluss beim IT-Dienstleister Xplain nach der Cyberattacke durch die Hackergruppe Play. Die Firma aus Interlaken wurde mutmasslich im Mai 2023 gehackt, in der Folge sind sensitive Informationen wie Sicherheitsdispositive oder andere heikle Daten im Darknet gelandet: etwa Personendaten von überwachten Schwerverbrechern oder Terroristen, aber auch solche von beliebigen Schweizern und Migrantinnen.

Was diesen Informationen gemeinsam ist: Sie hätten niemals in dieser Form bei einer privaten Firma landen dürfen, die eigentlich nur für den Betrieb der Software verantwortlich wäre.

Der Datenschutzbeauftragte leitete deshalb eine Administrativuntersuchung gegen die Bundesämter BAZG und Fedpol ein, der Bundesrat lässt die geschäftlichen Beziehungen zu Xplain genauer untersuchen. Der Verdacht: massive Vernachlässigung der Aufsichtspflicht bei der Datensicherheit. Ausserdem hat das Fedpol Strafanzeige gegen unbekannt eingereicht, die Bundesanwaltschaft ermittelt.

Es handelt sich wohl um den gravierendsten Cyberangriff in der Geschichte der Bundesverwaltung. Und das ganze Ausmass des Schadens ist noch nicht absehbar. Klar ist allerdings, dass diese Affäre weit über den Bund hinausreicht. Auch etliche Kantone haben Xplain-Produkte bezogen, wie Recherchen der Republik ergeben haben.

Während nun alle betroffenen Behörden mit Hochdruck daran arbeiten, sich ein vollständiges Bild von ihren verzweigten Verstrickungen mit dem Unternehmen aus dem Berner Oberland zu machen, zeigen unsere eigenen Nachforschungen:

1. Bei Beschaffungen wandten die Bundesverwaltung und die Kantone zahlreiche Tricks an, die **auf eine systematische Bevorzugung des Berner Unternehmens hindeuten.** Durch die vielen Zuschläge hat sich die Firma Xplain in eine Position gebracht, von der sie kaum mehr verdrängt werden konnte: Sie wurde *too big to fail*.
2. Aus unserer Analyse von Ausschreibungsunterlagen und Verträgen geht hervor: Besonders bei den Beschaffungen von 2008 bis 2018 machten die Behörden **kaum Vorgaben bezüglich der IT-Sicherheit** von Xplain-Produkten.
3. Einige Ämter wie das Fedpol und auch gewisse Kantone versuchen, **die Recherchen der Republik aktiv zu behindern,** und verweigern sogar Auskünfte zu Informationen, die früher öffentlich verfügbar waren. Damit geben sie indirekt einen Hinweis darauf, welche Frage bei den offiziellen Untersuchungen im Zentrum stehen dürfte: ob sie die Sicherheit der Xplain-Produkte überhaupt je getestet haben.
4.

Der Bund hält an der Zusammenarbeit mit Xplain fest, da sonst wichtige Gesetze nicht angewendet werden könnten. Ob aber eine neue iPhone-App zur Grenzkontrolle zum Einsatz kommen wird, ist ungewiss. **Damit steht ein wichtiges Schengen-Projekt auf der Kippe, zu dem sich die Schweiz verpflichtet hat.**

1. Die Beschaffungstricks: Irreführende Deklarationen, geheime Beschaffungen und zugeschnittene Ausschreibungen

Freihändige Vergaben – im Jargon auch «Freihänder» genannt – sind ein Dauerbrenner in der politischen und medialen Debatte. Sie bedeuten: Die Bundesverwaltung oder ein Kanton vergeben einen Auftrag ohne öffentliche Ausschreibung an eine Firma. Zulässig ist dies, wenn der Wert des Auftrags unterhalb von 150'000 Franken liegt.

In bestimmten Ausnahmefällen, welche im Beschaffungsrecht geregelt sind, können Aufträge unabhängig vom Schwellenwert freihändig vergeben werden: etwa wenn die Umstellung auf ein neues System «substanzielle Mehrkosten» mit sich brächte oder wenn es schlicht «keine angemessene Alternative» gibt.

Doch der öffentliche Sektor macht auffallend oft von diesem Mittel Gebrauch: Über die Hälfte der Zuschläge im IT-Bereich würden von den Behörden ohne offene Ausschreibung und somit ohne Wettbewerb «unter der Hand» vergeben, sagt Matthias Stürmer, Leiter des Instituts Public Sector Transformation an der Berner Fachhochschule. «Diese systematische Umgehung des Markts widerspricht zentralen Grundprinzipien des öffentlichen Beschaffungswesens, verhindert Innovation und führt letztlich zur Verschwendung von Steuergeldern.»

Die Verträge mit der Firma Xplain sind hier keine Ausnahme: Gemäss den Beschaffungsplattformen Simap.ch und Intelliprocure hat die Firma im Zeitraum von 2008 bis 2023 elf von zwanzig Aufträgen freihändig – also direkt und ohne Ausschreibung – erhalten.

Doch die Probleme reichen tiefer: Wegen zahlreicher Beschaffungstricks war das tatsächliche Auftragsvolumen nämlich noch grösser als auf den Plattformen ausgewiesen. Und auch die offenen Ausschreibungen erweisen sich zum Teil als Farce. Das zeigt sich an folgenden Beispielen:

Das Geschäftsverwaltungssystem «Orma», für welches das Fedpol Xplain den Zuschlag gegeben hatte, taucht auf Simap.ch erstmals im Jahr 2011 auf. Der Titel des Geschäfts lautet: «Anpassungen (...) und Upgrade von Lizenzen». Die Einkäuferin Fedpol verweigert der Republik die Auskunft, wann die Software ursprünglich beschafft worden ist. Aus internen Dokumenten geht jedoch hervor, dass Xplain im Jahr 2009 ein Produkt für das Projekt «Orma» offerierte. Doch von der ursprünglichen Anschaffung findet sich auf Simap.ch keinerlei Spur.

Dasselbe Muster zeigt sich auch bei einem anderen Geschäft: Gemäss öffentlichen Angaben hat das Zollamt die «Weiterentwicklung» des Abrufsystems «eneXs (mobile Version)» im Jahr 2013 freihändig bei Xplain eingekauft. Das Grenzwachtkorps nutzt «eneXs» für den Abgleich von Identitätsdokumenten mit unterschiedlichen Datenbanken. Mit dem Auftragstitel suggeriert die Bundesbeschaffungsbehörde, dass die Technologie Anpassungen benötige, die nur Xplain anbieten könne.

Doch wann hatte das Zollamt die Applikation ursprünglich beschafft? Und gab es dazu ein offenes Verfahren?

Die Erstbeschaffung der mobilen Version habe im Jahr 2013 stattgefunden, lautet die Antwort des BAZG. Das bedeutet: Unter falschem und irreführendem Titel («Weiterentwicklung und Wartung der Fachapplikation eneXs mobile») wurde hier ein Folgeauftrag vorgegaukelt, der eigentlich eine Erstbeschaffung war. Hinzu kommt: Das BAZG hat nach eigenen Angaben bereits das ursprüngliche System «eneXs» 2009 von Xplain entwickeln lassen. Doch auch das wird auf der Beschaffungsplattform Simap.ch nicht transparent gemacht.

Wie sich Xplain lukrative Folgeaufträge und langfristige Partnerschaften sichern konnte, zeigt sich auch im Kanton Aargau, der neben dem Fedpol und dem Bundesamt für Justiz zu den treusten Kunden von Xplain gehört. 2013 suchte der Kanton ein neues «Rapportierungssystem» und schrieb den Auftrag dafür öffentlich aus. Zwei Firmen offerierten, darunter Xplain. Die Berner Firma gewann den Grundauftrag im Wert von 750'000 Franken. Drei Jahre später, 2016, erhielt sie noch einmal 900'000 Franken bewilligt: für die Implementierung der Zusatzmodule «Kriminalpolizeiliches Informationssystem» und «Asservatenverwaltung».

Die Auftragssumme des Freihänders überstieg also diejenige des Grundauftrags, für den Xplain im Wettbewerb den Zuschlag erhalten hatte. Die freihändige Vergabe eines Auftrags sei gemäss der Gesetzgebung im Kanton Aargau zulässig, wenn dieser «in der Ausschreibung des Grundauftrages als geplante Erweiterung (...) mit freihändiger Vergabe an den Gewinner (...) angekündigt worden ist», steht in der Begründung auf Simap.ch. Der künftige, teurere Freihänder war also bereits miteinkalkuliert.

Das vierte und krasseste Beispiel, wie Xplain bei einer Ausschreibung bevorzugt wurde: Für einen Auftrag von 2021 mit dem Titel «Mobiles Grenzkontrollsystem» im Wert von 8,4 Millionen Franken gab es zwar eine offene Ausschreibung. Ein Angebot eingereicht hat allerdings nur eine Firma: Xplain.

Wer das Pflichtenheft liest, stellt fest: Xplain löste sich dabei selbst ab. Denn das zu ersetzende Vorgängerprodukt zur smarten Grenzkontrolle stammte ebenfalls von der Berner Firma.

Wurde dabei die Ausschreibung auf Xplain zugeschnitten? Der Schluss liegt nahe, denn für Newcomer-Firmen galten fast unüberwindbare Hürden. So verlangte die Beschaffungsbehörde bei den offerierenden Firmen folgende «Referenz»: ein Produkt, bei dem eine Anbindung der Datenbanken an bestehende Fahndungs- und Informationssysteme des Bundes bestehe. Ausserdem müsse es an das «Single-Sign-on-Portal des EJPD» angeschlossen sein, die Sicherheitsinfrastruktur des Departements. Und zuletzt: Bieterfirmen müssten eine iPhone-App vorweisen können, welche die Grenzkontrolle bei Abfragen zu aktuellen Fahndungen unterstützen könne.

All das konnte praktisch nur Xplain anbieten – mit ihrer eigenen Technologie, die nun abgelöst werden sollte: «eneXs mobile».

Auf Anfrage widerspricht die Bundesbeschaffungsbehörde: Es gebe «mindestens zwei» nationale Anbieter, die diese Kriterien erfüllten. Fakt ist: Offeriert hat am Ende nur Xplain.

Der Grundstein für die enge Verflechtung zwischen dem Bund und der Berner IT-Firma wurde bereits im Jahr 2008 gelegt. Damals beschaffte das Verteidigungsdepartement VBS für das Projekt «Jorasys» ein Rapport-

system für die Militärpolizei. Auch diese Anwendung wurde nun von der kriminellen Play-Gruppe gehackt. Unter anderem wurden die Namen der Mitglieder einer militärischen Sondereinheit entlarvt, die gezielt gegen ausländische Spione vorgeht, wie SRF berichtete.

In der Ausschreibung verlangte Armasuisse damals, dass die offene technische Schnittstelle zu allen polizeilichen Systemen wie etwa zu «automatisierten Fahndungssystemen» (also dem nationalen Fahndungssystem «Ripol») oder dem «Informationssystem der Bundeskriminalpolizei» («Janus») offeriert werde. Eine Anforderung, die Xplain bei ihren Offerten – die der Republik vorliegen – immer wieder zum eigenen Vorteil ausspielen konnte.

Insgesamt führte die Firma Xplain für den Bund, für Kantone und für die SBB bis heute gemäss Simap.ch Aufträge im Wert von mindestens 50 Millionen Franken aus.

Mindestens. Weil: Etliche weitere Aufträge an die Firma sind geheim erfolgt. Etwa für «Quattro P», ein ebenfalls gehacktes Informationssystem, mit welchem Grenzkontrollorgane dem Nachrichtendienst Daten übermitteln. Die Begründung des VBS für die freihändige Vergabe lautet so: «Vergaben, welche sich beispielsweise auf den Ausnahmeartikel zur Aufrechterhaltung der inneren und äusseren Sicherheit sowie der öffentlichen Ordnung beziehen, müssen nicht auf Simap.ch veröffentlicht werden.»

Die Kantone Zürich und Aargau sind ebenfalls emsige Einkäufer von Xplain-Produkten. Die Kantonspolizei Zürich nutzt das «eneXs»-Abrufsystem. Ein entsprechender Auftrag ist auf Simap.ch allerdings nicht auffindbar. Der Auftrag sei unterhalb der «Submissionslimite», sagt der Sprecher der Kantonspolizei Zürich. Gemeint ist: unterhalb der Beitragshöhe, die eine öffentliche Ausschreibung und einen offenen Wettbewerb verlangen würde. Ebenfalls nicht ausgeschrieben wurden gemäss der Republik vorliegenden Dokumenten Aufträge der Kantonspolizeien Bern, Basel-Stadt und Nidwalden, der Stadtpolizei Winterthur, des Universitätsspitals Basel und zahlreicher Gemeinden.

Beschaffungsexperte Matthias Stürmer sieht in all den Vergabetricks ein grundlegendes Problem: «Bei IT-Beschaffungen werden Systeme, die von einer Firma entwickelt wurden, leider meistens auch nur von dieser Firma mittels Freihänder über viele Jahre weiterentwickelt.» Wenn der öffentliche Sektor mehr auf frei verfügbare Software setzen würde, dann könnten auch andere Hersteller an diesen Systemen später weiterarbeiten, sagt er. Stürmer setzt seine Hoffnung auf das neue Embag-Gesetz, das 2024 in Kraft tritt und von der Bundesverwaltung verlangt, ihre Software unter Open-Source-Lizenzen zu veröffentlichen.

2. Lasche Vorgaben zur IT-Sicherheit

Es scheint so, dass sich die Bundesverwaltung erst nach dem Hack die Website eines ihrer wichtigsten IT-Dienstleister genauer angeschaut hat. Denn die Firma Xplain hatte in ihrer öffentlichen Webpräsenz nicht nur ihre Softwareprodukte beworben, sondern auch deren Kunden preisgegeben.

Unter «Referenzen» wurden Cyberkriminellen potenziell heikle Informationen auf dem Servierteller präsentiert: etwa welche Produkte der Kanton Aargau oder das Bundesamt für Justiz für die Strafverfolgung und damit für die Dokumentationen von Täterinnen nutzen. Auch wenn unklar ist, ob die Hackerbande Play wirklich erkannte, auf welche Schatztruhe sie mit den ungesicherten Servern der Firma Xplain gestossen war (schliesslich ga-

ben die Hacker im Darknet zuerst an, Datensätze von einem kommerziellen Dienstleister zu veröffentlichen, und verkauften diese wohl eher unbewusst unter Wert): Beim Fedpol und beim Zentrum für Cybersicherheit sorgte die Entdeckung der Xplain-Referenzen für Entsetzen, wie Insider berichten.

Xplain hat die Rubrik in der Folge entfernt, über Webarchive ist sie aber noch auffindbar. Wie eine Republik-Recherche vom Juli zeigt, verfügt Xplain zudem nicht über die nötigen Zertifizierungen für IT-Sicherheit.

Es erscheint fraglich, ob diese Zertifikate vonseiten des Bundes überhaupt je eingefordert worden sind. Und wie der Reality-Check bei der IT-Sicherheit allgemein ausgesehen hat. Denn Fakt ist: Die Cyberattacke geschah unter anderem wegen Versäumnissen aus dem Zeitraum 2008 bis 2018.

Schon der erste offizielle Bundesauftrag aus dem Jahr 2008, als Xplain die Technologie für das Rapportsystem für die Militärpolizei offerierte, wirft Fragen auf. Aus den Ausschreibungsunterlagen geht hervor, dass der Auftragnehmer «Weisungen zur Informatiksicherheit des Bundes» zu akzeptieren habe. Ausserdem wird von Armasuisse auf weitere Regularien wie die «Network Security Policy» oder eine «Informatikschutzverordnung» verwiesen (diese sind nicht mehr öffentlich verfügbar und können nur im Bundesarchiv eingesehen werden).

Doch ob und wie die Akzeptanz dieser Vorschriften schriftlich bezeugt und periodisch überprüft wurden, darüber verweigert das VBS mit Verweis auf die Untersuchungen die Auskunft (mehr dazu unter Punkt 3).

Ein weiteres Beispiel: 2015 kaufte das Bundesamt für Justiz bei Xplain ein Geschäftsverwaltungssystem mit dem Arbeitstitel «Pagirus». Die Republik fragte bei der Beschaffungsbehörde nach, welche Richtlinien für Datenschutz und Datensicherheit damals für Xplain gegolten hätten. Das Bundesamt für Bauten und Logistik verwies auf die Ausschreibungsunterlagen, die es aufgrund eines Gesuchs der Republik via Öffentlichkeitsgesetz herausgegeben hatte. Doch darin sind keine Regularien aufgeführt. Von Bundesseite wird lediglich die Mitwirkung an Dokumenten zu «Informationssicherheit und Datenschutz» gefordert. Und noch ein Beispiel für fehlende Verbindlichkeit: Gemäss «Le Temps» enthielt der Fedpol-Vertrag von 2011 für die Beschaffung von «Orma» keine Klausel über die notwendige Löschung von echten Daten.

Ab 2018 scheint der Wind gedreht zu haben: Der Bund forderte in den Verträgen verbindliche Checks zur regelmässigen Prüfung von Sicherheitslücken. Die fortschrittlichsten Bestimmungen gibt es beim Xplain-Projekt «Mobiles Grenzkontrollsystem». Ausgerechnet bei der Applikation, die noch gar nicht in Betrieb genommen wurde.

3. Wie der Bund Informationen verweigert – und damit seine mangelnde Aufsichtstätigkeit verrät

Die Nervosität in Bundesbern ist spürbar. Jeder Medienbeitrag über die Darknet-Files und Xplain sorgt für noch mehr politischen Druck. Das VBS beispielsweise entschied sich, in die Offensive zu gehen, und kommunizierte in eigener Sache, um einer SRF-Publikation zum Hack der Daten von Militärpolizistinnen zuvorzukommen. Dasselbe passierte auch der Republik. Unsere Fragen rund um den Passdaten-Abfragedienst «eneXs» veranlassten das Zollamt dazu, einen eigenen Artikel zu publizieren. Dieser wurde allerdings nicht als Medienmitteilung veröffentlicht, sondern unter der etwas versteckten Rubrik «Brennpunkt-Teaser».

Bereits vor Monaten hat die Republik via Öffentlichkeitsgesetz die Herausgabe sämtlicher Ausschreibungsunterlagen, Verträge und ISDS-Konzepte (Schutzkonzepte zur Informationssicherheit und zum Datenschutz) verlangt.

Die Bundesämter haben die Mehrheit der Gesuche abgelehnt. Besonders verschlossen zeigte sich das Fedpol.

Laura Marinello, die Chefin der Abteilung Recht und Massnahmen beim Fedpol, begründet die ablehnende Antwort folgendermassen: «Die von Ihnen angefragten Unterlagen und Informationen stehen in Zusammenhang mit den laufenden Verfahren (Strafverfahren der Bundesanwaltschaft, formelle Untersuchung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten sowie Administrativuntersuchung des Bundesrates).»

Das Bundesamt für Polizei verweigerte auch auf simple Nachfragen Antworten, ebenso Armasuisse. Damit werden Medien aktiv an ihren Recherchen behindert. Besonders stossend daran ist, dass selbst die Herausgabe von ehemals öffentlichen Informationen wie Ausschreibungsunterlagen verweigert wird.

Eine Ausnahme bildet das Bundesamt für Zoll und Grenzsicherheit (BAZG), das Fragen durchaus beantwortet und ein Gesuch um Einsicht umfangreich bearbeitet hat. Allerdings nur in Bezug auf jenes Xplain-Produkt, das nicht gehackt worden ist, weil es noch gar nicht in Betrieb genommen wurde: das «Mobile Grenzkontrollsystem».

Die übrige Bundesverwaltung dagegen verrät mit ihrer Informationsblockade unfreiwillig, welche Ursache das Datenleck bei Xplain gehabt haben dürfte. So haben die Behörden die Herausgabe der Informationsschutzkonzepte für das Abrufsystem «eneXs» – die Plattform für die Prüfung von Pässen und Identitätskarten – verweigert; mit Verweis auf die laufenden Untersuchungen. Dasselbe gilt für IT-Sicherheitskonzepte, Abnahmeprotokolle sowie Test- und Auditberichte der Aufträge zu «Jorasys», «Janus» und «Orma» – allesamt Xplain-Produkte, die von der Bande Play gehackt worden sind, wodurch teilweise höchst sensible Personeninformationen im Darknet gelandet sind. Gemäss «Tages-Anzeiger» sollen zumindest das Fedpol und die Zollverwaltung gar nie Audits durchgeführt haben.

Es ist daher unklar, ob die Vorgaben zur IT-Sicherheit überhaupt jemals ernsthaft überprüft worden sind.

4. Schengen-Projekt auf der Kippe

Die Republik-Recherchen zeigen ausserdem: Die Produkte von Xplain sind für den Bund mittlerweile systemrelevant geworden. Ohne diese Technologien müssten viele der laufenden Bundesprojekte sofort gestoppt werden. Das Geschäftsverwaltungssystem «Orma» etwa wird in internen Dokumenten zum Programm «FMÜP P4», zum offiziellen Überwachungsprogramm, das «zentrale Subsystem» genannt. Es enthält zum Beispiel die Daten zu Personen, die derzeit gerade überwacht werden oder gegen die eine Massnahme verhängt worden ist. Um das heutige Überwachungsgesetz Büpf oder das Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT) anzuwenden, wird auf Xplain-Software zurückgegriffen.

Doch geniesst Xplain überhaupt noch das Vertrauen der Bundesverwaltung?

Fedpol-Mediensprecher Christoph Gnägi hält fest, dass die geleakten Datensätze aus der Vergangenheit stammen und die aktuellen Daten auf einer isolierten Umgebung unter Hoheit des Bundes gespeichert sind. Er betont: «Gehackt wurde die Firma Xplain, nicht die Systeme von Fedpol. Die von Fedpol betriebenen Informationssysteme und Datenbanken laufen auf einer gesicherten Infrastruktur des Bundes.»

Klar scheint aber auch: Aufgrund der vielen gesetzlichen und technischen Sachzwänge haben die Sicherheits- und Strafverfolgungsbehörden wie Fedpol oder das Bundesamt für Justiz derzeit gar keine andere Möglichkeit, als an der Zusammenarbeit mit Xplain festzuhalten.

Und wie sieht es mit Zukunftsprojekten aus?

Die noch nicht lancierte App «Mobiles Grenzkontrollsystem» ist Teil des «Smart Borders»-Projekts der Schengen-Länder, zu dem sich auch die Schweiz verpflichtet hat. Sie bildet den technologischen Teil des «Entry/Exit System» ab. Mit dem Schengen-Projekt sollen die Ein- und die Ausreise von Personen aus Drittstaaten in den und aus dem Schengen-Raum registriert und deren Name, Geburtsdatum, Fingerabdrücke und ein Gesichtsbild gespeichert werden. Dadurch kann das Bundesamt für Zoll und Grenzsicherheit eine Liste aller *overstayers* erstellen, also der Personen, die theoretisch wieder ausreisen müssten.

Gemäss Anfrage beim BAZG ist die Firma Xplain bei diesem Projekt zumindest noch nicht abgeschrieben. Es seien «diverse Abklärungen im Gange, die daraus resultierenden Erkenntnisse werden laufend analysiert», schreibt das BAZG auf Anfrage. Ob der Bund rechtlich betrachtet überhaupt die Möglichkeit hätte, aus dem Vertrag mit Xplain auszusteigen, ist eine offene Frage.

Fazit

Viele Zuschläge an den IT-Dienstleister Xplain basieren auf technologischen Pfadabhängigkeiten: Die Firma war bereits in den frühen Nullerjahren im Markt der IT-Dienstleister für Sicherheitsbehörden präsent und konnte danach ihre Software sukzessive an die Informationssysteme des Bundes andocken.

Die Xplain-Produkte waren irgendwann so eng mit der IT-Systemlandschaft der Sicherheitsbehörden verflochten und das Management der Berner Firma so eng mit Departementen und Ämtern wie dem Fedpol, dem VBS oder dem Bundesamt für Justiz vernetzt, dass jede neue Ausschreibung quasi zum Heimspiel wurde. Die Referenzliste war lang und die Standards wurden praktisch durch das Berner Unternehmen selbst gesetzt. Damit wurde Xplain zu einem Klumpenrisiko für den Bund.

Dieser Vertrauensvorschuss führte zu Nachlässigkeit bei den Behörden. Sie haben es sträflichst versäumt, bei einem ihrer wichtigsten IT-Dienstleister verbindliche Vorgaben zu Datenschutz und IT-Sicherheit zu machen und deren Einhaltung zu kontrollieren. Das Nationale Zentrum für Cybersicherheit ist in den letzten Monaten nun über die Bücher gegangen und hat an alle IT-Dienstleister, die aktuell eine Leistungsvereinbarung mit der Bundesverwaltung haben, einen Brief verschickt. Darin weist das Kompetenzzentrum alle Partnerfirmen an, die Hausaufgaben in Sachen Cybersecurity zu machen.

Wäre das bloss 10 Jahre früher geschehen.

In einer früheren Version haben wir das Stadtrichteramt Zürich in einer Reihe von kommunalen und kantonalen Ämtern aufgezählt, die freihändig Aufträge an Xplain vergeben haben. Das Stadtrichteramt Zürich hat die Beschaffung jedoch in einem offenen Verfahren durchgeführt mit Xplain als Sublieferantin.