Datenklau: Xplain arbeitete auch für den Nachrichtendienst

Der Hackerangriff wirft heikle Fragen auf – für die betroffene Schweizer IT-Firma genauso wie für Bundesbehörden. Eine Auslegeordnung in zwölf Punkten.

Von Basil Schöni, 11.07.2023

Bundesbern ist im Stress. Seit dem Hackerangriff auf die Schweizer IT-Firma Xplain tauchen im Darknet sensible Daten des Bundes auf. Die Behörden geben sich bedeckt. Informationen über Art und Umfang der Daten gelangen bloss in Bruchstücken – und zum Teil nicht der Wahrheit entsprechend – an die Öffentlichkeit.

Die Republik hat sich den Datensatz angeschaut. Resultat der Recherche: Erstens befinden sich unter den gehackten Daten auch solche, die mit dem Nachrichtendienst des Bundes (NDB) zu tun haben. Und zweitens stellen die bisher veröffentlichten Daten möglicherweise nicht einmal die Hälfte von dem dar, was tatsächlich gestohlen wurde.

Wie bitte? Nachrichtendienst?

Ja, tatsächlich. Aus einem Dokument von Xplain geht hervor, dass die IT-Firma verschiedene Verträge abgeschlossen hatte, die das Informationssystem «Quattro P» betreffen. Dieses System enthält Personendaten, die die Grenzkontrollorgane dem Nachrichtendienst übermitteln. Der Nachrichtendienst überwacht damit, wann «bestimmte Kategorien von ausländischen Personen» (so die Formulierung im Nachrichtendienstgesetz) die Schweizer Grenze übertreten.

In den veröffentlichten Daten zu Quattro P sind auch einzelne operative Informationen enthalten. So finden sich sechs Dateien, die Xplain wohl als Beispiele dienten, wie Daten über Ein- und Ausreisen ausgetauscht werden. Jede dieser sechs Dateien dokumentiert einen Grenzübertritt einer Person. Enthalten sind Informationen wie Name, Geburtsdatum, Passnummern, Datum der Ein- oder Ausreise sowie verschiedene Fotos der Reisepässe der betroffenen Person.

Ob die sechs Personen aus Serbien, den Vereinigten Arabischen Emiraten, Pakistan und dem Iran im Visier des Schweizer Nachrichtendienstes sind, lässt sich aufgrund der vorliegenden Daten nicht beurteilen.

Auf jeden Fall ist es heikel, wenn eine private Firma an der Entwicklung eines Informationssystems beteiligt ist, mit dem der Geheimdienst Personen überwacht. Ausserdem stellt sich die Frage, welchen Zugang die IT-Firma zu den operativen Daten in Quattro P hatte.

Es bleibt zu hoffen, dass nicht noch mehr Daten zu Quattro P gestohlen wurden als die wenigen Informationen, die die Hackergruppe Play bisher veröffentlicht hat. Das ist aber keineswegs garantiert. Denn die Hacker könnten noch weit mehr Daten haben als jene, die sie vor einigen Wochen ins Darknet gestellt haben.

Es könnte also sein, dass noch nicht alle gestohlenen Daten veröffentlicht wurden?

Es gibt Hinweise, dass das so ist.

Die Gruppe Play schreibt auf ihrer Website von 907 Gigabyte, die sie angeblich veröffentlicht hat. Verschiedene Zeitungen übernahmen diese Behauptung. Doch die Zahl stimmt nicht. Die Daten, die die Hacker bisher veröffentlicht haben, umfassen nur rund 400 Gigabyte. Das bestätigte gegenüber der Republik auch das National Cyber Security Centre (NCSC), das nationale Zentrum für Cybersicherheit.

Für diesen Unterschied gibt es drei Erklärungsansätze.

Einerseits kann es sein, dass die Zahl, die Play kommuniziert hat, von Anfang an falsch war. Tatsächlich sind die von Play kommunizierten Zahlen manchmal unscharf. So bietet Play auf seiner Website vereinzelt Datensätze zum Download an, deren Umfang sehr viel geringer ist als die Zahl, welche die Hacker angeben. In anderen Fällen sind die Datensätze sogar etwas grösser als die von Play genannten Zahlen. Bei den meisten Datensätzen stimmt der Umfang der downloadbaren Datensätze aber ungefähr mit den Angaben von Play überein. Es ist also möglich, dass die von Play genannten 907 Gigabyte schlicht falsch sind und die Hacker tatsächlich nur knapp 400 Gigabyte besitzen. Die meisten von Play genannten Zahlen scheinen aber zuzutreffen.

Eine zweite Möglichkeit ist, dass Play aus Versehen nicht alle Daten hochgeladen hat. Dagegen spricht aber die Struktur der veröffentlichten Dateien. Die Hacker stellen den Datensatz als eine Reihe von Dateiarchiven (ähnlich dem Zip-Format) zur Verfügung. Die letzte dieser Dateien ist kleiner als die 645 vorherigen. Das deutet darauf hin, dass die publizierten 400 Gigabyte als Ganzes verpackt und veröffentlicht wurden.

Schliesslich kann es auch sein, dass Play absichtlich nicht alle Daten hochgeladen hat. Dann hätte die Hackergruppe gezielt mehr als die Hälfte des Datensatzes zurückbehalten. Ein solches Vorgehen könnte verschiedene Gründe haben. Vielleicht erfolgte im Hintergrund doch noch eine Lösegeldzahlung. Oder Play hat die Daten anderweitig verkauft oder weitergegeben. Das wäre für die Schweiz der Worst Case.

Eine klare Aussage lässt sich mit dem heutigen Wissensstand nicht machen. Es ist aber durchaus realistisch, dass Play noch deutlich mehr Daten besitzt als bisher öffentlich bekannt. Genaueres könnten hier wohl die Bundesbehörden sagen. Es ist anzunehmen, dass diese Zugriff auf den Server von Xplain haben, von dem die Daten gestohlen wurden. Falls dort Daten gespeichert waren, die bisher noch nicht veröffentlicht wurden, muss angenommen werden, dass das Ausmass des Schadens noch deutlich grösser ist als bisher kommuniziert.

Das nationale Zentrum für Cybersicherheit NCSC wollte dazu auf Anfrage keine Auskunft geben.

Und die Daten, die schon ins Darknet gestellt wurden? Was für Informationen sind dort genau drin?

Bis jetzt sind acht Fälle von sensiblen Daten bekannt, die von Play veröffentlicht wurden:

- Acht Dokumente des Bundes, die als «Vertraulich», sowie mindestens vierzehn, die als «Intern» klassifiziert sind.
- Unter diesen Dokumenten sind auch mehrere Dateien des Bundesamts für Polizei Fedpol, die Sicherheitsmassnahmen für besonders gefährdete Orte, Anlässe und Personen enthalten. Darunter findet sich eine Liste mit 63 diplomatischen Vertretungen, Bundesgebäuden und Bundesratsresidenzen im Kanton Bern samt Adressen, Gefährdungseinschätzung und Sicherheitsmassnahmen. In dieser Datei sind auch die Wohnadressen verschiedener Bundesräte und hoher Bundesbeamter enthalten. Die Daten stammen aus der Zeit von August 2017 bis März 2018.
- Mehrere Excel-Dateien, aus denen Namen, Abteilung, Kommissariat und IT-Berechtigungen von Mitarbeitenden der Bundeskriminalpolizei ersichtlich sind. Insgesamt sind mehrere hundert Personen betroffen. Die Daten stammen von März bis Oktober 2022.
- Verschiedene Excel-Dateien, die Daten des Amts für Migration und Integration des Kantons Aargau enthalten. Betroffen sind Name, Geburtsdatum, Zivilstand, Staatsangehörigkeit, Geschlecht, Passnummer, Kontonummern und weitere Informationen von Personen, die sich vermutlich in einem Migrationsverfahren befinden.
- Mehrere Excel-Dateien mit Daten von Personen, die bei den SBB Hausverbote bekommen haben. Sie beinhalten unter anderem Namen, Geburtsdatum sowie Grund und Datum des Hausverbots.
- Wie der «SonntagsBlick» meldete, sind auch Fahndungsausschreibungen von Interpol, sogenannte *Red Notices,* in dem Datensatz enthalten. Die Republik konnte das bis Redaktionsschluss nicht abschliessend bestätigen. Zwar findet sich im Datensatz eine Datei, die die Aufhebung von fünf *Red Notices* dokumentiert. Ob sich der «SonntagsBlick» mit seiner Meldung auf diese Datei bezieht, ist aber unklar.
- Weiter schreibt der «SonntagsBlick», dass womöglich Log-in-Daten zu Systemen der Bundesverwaltung gestohlen wurden.
- Schliesslich meldete die NZZ mit Verweis auf Quellen aus der Bundesverwaltung, dass auch Haftbefehle oder Verhörprotokolle öffentlich gemacht wurden.

Weil der Datensatz sehr viele Dateien enthält und diese nur mit einem gewissen Aufwand gründlich durchsucht werden können, ist es gut möglich, dass noch weitere sensible Daten auftauchen werden. Und da die veröffentlichten 400 Gigabyte möglicherweise nicht den ganzen gestohlenen Datensatz darstellen, kann es zudem sein, dass die Hackergruppe noch weitere heikle Dokumente besitzt.

Es ist aber klar, dass die operativen Daten der Xplain-Kunden nur einen kleinen Teil des Datensatzes umfassen. Der grösste Teil setzt sich aus Dokumenten zusammen, die der Planung und Umsetzung der zu entwickelnden Software dienten. Also Dinge wie Konzepte, Spezifikationen, Präsentationen und so weiter. Daneben finden sich auch administrative Dokumente der Firma Xplain wie Verträge, Protokolle von Mitarbeitergesprächen, Versicherungspolicen und Ähnliches. Auch private Daten der Xplain-Mitarbeitenden, die gar nichts mit ihrer Arbeit zu tun haben, sind teilweise betroffen.

Wie konnten solch sensible Daten bei Xplain landen?

Das ist noch Gegenstand der Untersuchungen des Bundes. Xplain erledigte für den Bund, für die SBB und für verschiedene kantonale Behörden zahlreiche IT-Aufträge. Bei manchen der veröffentlichten heiklen Daten legen Beschriftungen und Ordnerstrukturen gewisse Ursachen nahe:

- Die SBB-Hausverbote befinden sich in einem Ordner namens «Support», die Dateien tragen alle die Zeichenkette «export_hausverbotetodelete» im Namen. Das deutet darauf hin, dass Xplain von ihrer Kundin den Auftrag erhielt, gewisse Hausverbote aus der Datenbank zu löschen. Vermutlich hat eine Mitarbeiterin dann eine Arbeitskopie der zu löschenden Einträge erstellt und diese nicht mehr gelöscht.
- Die Fedpol-Dokumente, die Sicherheitsmassnahmen enthalten, liegen in einem Ordner, dessen Name darauf hindeutet, dass es sich dabei um Beispieldateien handelt. Diese Beispiele sollten Xplain wohl zeigen, wie derartige Dokumente aufgebaut sind, damit die Firma selber mit solchen Informationen arbeiten kann.
- Die Tabellen, die Mitarbeiterinformationen der Bundeskriminalpolizei enthalten, befinden sich in einem Ordner namens «FEDPOL REORG BKP». In diesem Ordner findet sich auch eine Präsentation, die die Neuorganisation der Bundeskriminalpolizei beschreibt. Verschiedene Abteilungen und Kommissariate wurden zusammengelegt oder anderweitig neu organisiert. In den Excel-Dateien selber gibt es Spalten, die den Mitarbeiterinnen ihre bisherigen und neuen Abteilungen und Kommissariate zuordnen. Am wahrscheinlichsten ist, dass Xplain diese Reorganisation auf der Datenbank, die sie für die Bundeskriminalpolizei betreibt, abbilden musste und zu Arbeitszwecken diese Tabellen generiert hat.

Bei anderen heiklen Daten, wie beispielsweise jenen des Aargauer Amts für Migration und Integration, lassen sich keine verlässlichen Rückschlüsse ziehen. Vielmehr handelt es sich wohl um Arbeitskopien, die für die Weiterentwicklung der Software gebraucht und dann nicht wieder gelöscht wurden.

Das tönt alles nicht so gut. Wer hat denn Zugang zu diesen Daten?

Die Daten von Xplain wurden im Darknet publiziert. Das Darknet ist ein Teil des Internets, der nur über den sogenannten Tor-Browser erreichbar ist. Der Tor-Browser dient dazu, anonym im Internet zu surfen, und ist von zentraler Bedeutung in Ländern, wo das Internet stark zensiert ist oder Menschen aus anderen Gründen auf Anonymität angewiesen sind. Als Nebeneffekt ist Tor aber auch für kriminelle Aktivitäten attraktiv.

Wer in der Lage ist, den Tor-Browser auf seinem Computer zu installieren und den Link zur Website von Play findet, kann die Daten ohne weiteres herunterladen. Wegen des grossen Umfangs der Daten und weil die Anonymisierung des Tor-Browsers auf die Downloadgeschwindigkeit schlagen kann, dauert es aber ziemlich lange, alle Dateien herunterzuladen.

Und sind die Daten immer noch verfügbar? Kürzlich hiess es doch, sie seien verschwunden.

Anfang Juli meldete die Nachrichtenagentur Keystone-SDA mit Verweis auf das Nationale Zentrum für Cybersicherheit, dass die Daten aus dem Darknet verschwunden seien. Das stellte sich aber rasch als Falschmeldung

heraus. Die Nachricht hatte sich verbreitet, weil die Download-Website für einige Zeit nicht verfügbar war. Das war aber keineswegs ungewöhnlich: Seit Play die vollständigen Daten am 14. Juni veröffentlicht hatte, war die Seite immer wieder vorübergehend nicht erreichbar. Das machte das Herunterladen der Daten zwar mühsamer, verhinderte es aber nicht.

Okay, aber wer sind diese Hacker? Was ist ihre Motivation?

Die Daten von Xplain wurden auf der Darknet-Seite von «Play» veröffentlicht. Es wird vermutet, dass es sich dabei um eine Gruppe aus Russland handelt. Solche Hackergruppen arbeiten nicht für den russischen Staat, werden aber geduldet, solange sie keine inländischen Ziele angreifen.

Play ist eine sogenannte Ransomware-Gruppe. Solche Gruppen dringen in Computersysteme ein, um Daten zu entwenden und zu verschlüsseln. Noch vor einigen Jahren war das hauptsächliche Geschäftsmodell, dass das Opfer durch die Verschlüsselung keinen Zugriff mehr auf seine eigenen Daten hatte. Wollte es die Daten zurückhaben, musste es ein Lösegeld zahlen.

Als dieses Vorgehen verbreiteter wurde, haben viele Firmen reagiert. Mit regelmässigen Back-ups konnten sie den Zugang zu ihren Daten gewährleisten, auch wenn diese durch einen Angreifer verschlüsselt wurden. Die Ransomware-Gruppen sind darum dazu übergegangen, mit der Veröffentlichung der Daten zu drohen. Das Lösegeld sollte dann verhindern, dass interne Daten an die Öffentlichkeit gelangen und einen Reputationsschaden verursachen.

Das ist nun auch der Firma Xplain passiert. Weil sie zumindest für die erste Hälfte der entwendeten Daten kein Lösegeld zahlte, landeten die Daten im Darknet, wo sie nun jede interessierte Person (mit ein bisschen technischem Know-how) runterladen kann.

Warum traf es gerade die Bundesverwaltung? Hat Play gezielt den Schweizer Staat angegriffen?

Play hat nicht die Bundesverwaltung, sondern die IT-Firma Xplain angegriffen. Es erscheint dabei eher unwahrscheinlich, dass die Gruppe von den staatlichen Daten bei Xplain wusste. Der Xplain-Datensatz ist einer von mittlerweile 135, die Play innerhalb von acht Monaten veröffentlicht hat. Obwohl er klassifizierte Dokumente von Sicherheitsbehörden enthält, wird er auf der Darknet-Seite von Play genau gleich präsentiert wie beispielsweise die Daten einer Metallverarbeitungsfirma. Dass der Staat betroffen ist, erwähnt Play mit keinem Wort. Von einer Gruppe, die grösstmöglichen Imageschaden anrichten will, wenn ein Opfer das Lösegeld nicht bezahlt, würde man aber erwarten, dass sie solche Informationen offensiv kommuniziert – falls sie denn davon weiss.

Wahrscheinlich geriet Xplain ins Visier, weil sich Play generell für IT-Firmen interessiert. Dass dabei sensible Daten von Schweizer Sicherheitsbehörden gestohlen wurden, dürfte also eher ein Zufallstreffer gewesen sein. Politische Gründe für den Hack sind nicht naheliegend.

Wurde ein Lösegeld bezahlt?

Vermutlich nicht. In einem Interview mit dem «Tages-Anzeiger» sagte der Delegierte des Bundes für Cybersicherheit, dass Xplain kein Lösegeld be-

zahlt habe und auch keine solchen Forderungen an den Bund gestellt worden seien. Ob im Hintergrund nicht doch Gelder flossen, lässt sich natürlich nicht sagen. Eine solche Zahlung stünde unter höchster Geheimhaltung. Denn würde bekannt, dass die Schweiz Lösegelder für Daten bezahlt, wäre sie fortan besonders attraktiv für Ransomware-Gruppen.

Meldungen über Cyberangriffe in der Schweiz häufen sich. Hat der Xplain-Hack etwas damit zu tun?

Vergangenen Frühling schlug der Hackerangriff auf CH Media grosse Wellen, von dem auch die NZZ betroffen war. In den Tagen vor dem Videoauftritt des ukrainischen Präsidenten Selenski im Schweizer Parlament hatten diverse Websites des Bundes sowie von Post, SBB und weiteren exponierten Akteuren mit Verfügbarkeitsproblemen zu kämpfen. Ausserdem wurden in den letzten Jahren immer wieder Schweizer Firmen und Gemeindeverwaltungen Opfer von Cyberangriffen.

Bei den Vorfällen rund um die Selenski-Rede handelte es sich um sogenannte «Denial of Service»-(DoS-)Angriffe. Dabei wird gezielt die Verfügbarkeit eines Dienstes (beispielsweise die Website eines Bundesamts) eingeschränkt, indem der Server mit Anfragen überflutet wird. Daten können dabei aber nicht gestohlen werden. Die Folge ist bloss, dass eine Dienstleistung vorübergehend nicht verfügbar ist. Zu den Angriffen im Vorfeld der Selenski-Rede hatte sich die prorussische Hackergruppe «No Name» bekannt und sich explizit auf die Videoschaltung mit dem ukrainischen Präsidenten bezogen. Die damaligen Angriffe dürften die Schweiz also gezielt und aus politischen Gründen getroffen haben.

Anders sieht es bei den Hacks bei Xplain, CH Media und den diversen weniger aufsehenerregenden Angriffen der letzten Jahre aus. Zwar steckt hinter dem Hack bei CH Media ebenfalls die Gruppe Play. Einen speziellen Fokus auf die Schweiz hat diese aber nicht. Sie veröffentlichte im gleichen Zeitraum diverse Datensätze, beispielsweise aus den USA, Kanada, Deutschland, Spanien oder Frankreich. Die Zunahme solcher Ransomware-Angriffe in der Schweiz ist vielmehr Teil eines allgemeinen Trends. Dass angesichts einer global zunehmenden Zahl an Angriffen auch die reiche Schweiz in den Fokus von Lösegelderpresserinnen gerät, erstaunt nicht.

Was sind die Folgen dieses Angriffs? Was lernt die Schweiz daraus?

Das ist bis jetzt noch nicht klar. Der Bundesrat hat einen Krisenstab eingesetzt, der das weitere Vorgehen koordinieren soll. Zudem seien bereits erste Massnahmen getroffen worden, die aber nicht konkret benannt wurden. Weiter wird es eine Administrativuntersuchung geben zur Frage, ob Xplain die Sicherheitsvorgaben des Bundes unzureichend umgesetzt hat. Und bestehende Verträge mit Informatikdienstleistern sollen überprüft werden. Ausserdem haben sowohl Xplain als auch das Fedpol und das Bundesamt für Zoll und Grenzsicherheit Strafanzeige erstattet. Die Analyse der gestohlenen Daten dauert derweil noch an.

Und wer ist überhaupt schuld an dem Schlamassel?

Bis jetzt ist noch nicht geklärt, wie die Hacker in die Systeme von Xplain eindringen konnten. Die Tatsache, dass Xplain klassifizierte Daten des Bundes auf ihrem Server rumliegen liess, spricht jedenfalls nicht dafür,

dass die Firma ordentliche Prozesse für den Umgang mit derartigen Daten definiert hatte. Wie Xplain auf Anfrage der Republik bestätigte, verfügt die Firma auch über keine der einschlägigen Zertifizierungen für IT-Sicherheit.

Die ganze Schuld Xplain anzulasten, wäre aber verfehlt. Wenn das Fedpol einer privaten Firma vertrauliche Dokumente als Beispieldateien liefert, statt hierfür ein Dokument mit bedenkenlosen Testdaten zu füllen, hat das Bundesamt selber einen grossen Teil der Verantwortung zu tragen.

Generell lagert der Staat die Entwicklung grosser Teile seiner IT-Infrastruktur an private Firmen aus. Gegenüber SRF sagte Florian Schütz, der Delegierte des Bundes für Cybersicherheit, dass das nicht anders gehe, weil die Bundesverwaltung die nötigen Fähigkeiten gar nicht habe, um solche Dinge selber zu entwickeln.

Angesichts des Xplain-Hacks stellt sich die Frage, ob es nicht an der Zeit wäre, dass der Staat sich dieses Wissen endlich aneignet. Oder zumindest besser kontrolliert, wie private Dienstleister seine Daten schützen.

Transparenzhinweis: Auf Bitte des Fedpol haben wir den Namen eines Ordners im veröffentlichten Datensatz entfernt und durch eine Umschreibung ersetzt. Grund dafür sind Sicherheitsüberlegungen der Bundesbehörden.