Basler Ermittler gegen die globale Cyberkriminalität

Seit drei Jahren verfügt die Basler Staatsanwaltschaft über das Dezernat Digitale Kriminalität. IT-Fachleute und Kriminalpolizisten verfolgen von der Heuwaage aus Verbrecher im Internet. Ein Job, für den starke Nerven ebenso unabdingbar sind wie starke Rechner.

Cyberkriminalität ist längst kein Randphänomen mehr: Die Basler Staatsanwaltschaft ermittelt

Jonas Hoskyn

In den Büros ist es warm, und es liegt an mehr als nur an der schwülen Sommerluft. «Das sind unsere Computer», erklärt Andreas Sutter. Der 43-Jährige leitet seit drei Jahren das Dezernat Digitale Kriminalität (DDK) bei der Basler Staatsanwaltschaft. Für ihre Arbeit brauchen seine Leute hochgerüstete PCs, die man eher im Zimmer eines computerspielenden Teenagers erwarten würde als in Räumlichkeiten der Kriminalpolizei. «Bei unserer Arbeit benötigen wir grosse Rechen- und Speicherleistung», sagt Sutter. Die Arbeit: Das sind Themen wie Sextortion, Ransomware oder DoS-Attacken – also Erpressung etwa mit Nacktfotos, durch Verschlüsselung von Computern oder das gezielte Lahmlegen von Internetdiensten. Straftaten aus der digitalen Welt, die immer mehr in den öffentlichen Fokus rücken. Deshalb hat auch die Basler Regierung die Bekämpfung der Cyberkriminalität in ihren aktuellen Legislaturplan aufgenommen.

Vor Sutters Start hatten zwei Staatsanwälte die digitale Kriminalität im Nebenamt erledigt. «Wir haben festgestellt, dass man das Thema stärker ausleuchten muss. Es brauchte mehr Leute und Ressourcen, um der Entwicklung gerecht zu werden», sagt Martin Schütz, Sprecher der Basler Staatsanwaltschaft. Das Resultat war die neu geschaffene Abteilung mit rund einem Dutzend Ermittlern nur für die digitale Welt. Zusammengesetzt aus Kriminalpolizisten mit einem Faible fürs Digitale und Informatikern mit Interesse an Ermittlungsarbeit. Polizeilicher Spürsinn und technisches Verständnis sind entscheidend für den Erfolg.

Mühsames Zusammentragen von digitalen Puzzleteilchen

«Solche Leute findet man nicht einfach so», sagt Sutter. Zumal auch in der Privatwirtschaft digitale Forensik-Abteilungen angesichts der weltweiten Hackerattacken zurzeit massiv ausgebaut werden. Sutter selber vereint die verschiedenen Welten: Der 43-Jährige hat eine Lehre als Software-Programmierer absolviert. Nach dem anschliessenden Jusstudium an der Universität Basel leitete er ein KMU im IT-Bereich. Kurz bevor er zu alt dafür wurde, begann er nochmals von vorne und absolvierte ab 2016 die Polizeischule – «das war ein Bubentraum», sagt er. Es folgten vier Jahre Dienst, davon zwei Jahre Alarmpikett auf dem Claraposten. Diese drei Stränge seiner Ausbildung konnte er beim neuen Job bündeln.

Die Stärke seiner Abteilung sieht Sutter im Beitragen von Puzzleteilchen für andere. Etwa bei international agierenden Hackerbanden oder Kinderpornografie-Ringen, wo Basel einer von vielen Tatorten ist. Oder aber weniger spektakulär: bei der fachlichen Unterstützung der Kolleginnen und Kollegen der Basler Staatsanwaltschaft. Wenn eine Sonderkommission gebildet wird, etwa bei einem Tötungsdelikt, ist immer jemand vom DDK mit dabei. Mehr als die Hälfte der Arbeit des Dezernats Digitale Kriminalität besteht daraus, bei analogen Verbrechen digitale Spuren zu sichern und auszuwerten: Smartphones von Drogendealern, Festplatten von Pädokriminellen, Internetchatverläufe nach einem Beziehungsdelikt.

Komplizierte Geldflüsse in der Welt der Kryptowährungen

Hunderte von Ladekabeln hängen an der Wand im Büro der digitalen Forensik. Denn wenn ein Handy beschlagnahmt wird, ist es deutlich schwieriger, dieses auszulesen, wenn der Akku schlapp gemacht hat. Wie lange es dauert, bis die Ermittler tatsächlich an die Daten auf dem Smartphone rankommen, unterscheidet sich stark nach Modell. Zwischen einem Tag und mehreren Jahren ist alles möglich. Mit jedem Update von Apple oder Android beginnt das digitale Wettrüsten von neuem. Ein paar Zimmer weiter bedient sich die Abteilung digitale Ermittlung auch deutlich weniger spektakulärer Methoden. Hier werden Informationen zusammengetragen, die im Internet ohne Hürden zu finden sind, auf Websites, in sozialen Netzwerken, in Datenbanken und ähnlichem.

Eine Welt für sich ist auch das Krypto-Center der Basler Staatsanwaltschaft. Die beiden jüngsten Mitglieder der Kriminalpolizei – zwei Informatiker im Alter von 22 und 25 Jahren – verfolgen hier bei einem Straftatverdacht die Finanzströme der digitalen Währungen. Bei Internetdelikten wird meist auf eine Kryptowährung wie etwa Bitcoin gesetzt. Lange galt diese unter Cyberkriminellen als kaum nachverfolgbar. Drogenumschlagplätze im Darknet setzten auf die kaum regulierten Geldströme. Mittlerweile sind die Spiesse weniger ungleich: Während Digitalwährungen verbreiteter wurden, nahm auch die Regulierung zu. So finden die Ermittler mit Geduld meist einen Ansatz, um sich an die Fersen der Besitzer zu heften. Auch wenn diese dann oft am anderen Ende der Welt sind. Ein Mitarbeiter ist speziell für Rechtshilfegesuche ins und aus dem Ausland zuständig – von Russland bis Südkorea.

Die Täter kommen kaum je vor ein Basler Gericht

Praktisch jeder Fall stellt die Ermittler vor neue Herausforderungen. Denn die Täter agieren meist international, sind technisch auf dem neusten Niveau und müssen sich an keine Regeln halten. «Es ist ein Tüfteln, etwas zu finden, an das der andere nicht gedacht hat, auch wenn er noch so schlau ist», sagt Sutter. «Man muss immer wieder neue Sachen lernen und wissbegierig sein.» Zumal auch seine Kolleginnen und Kollegen von der «analogen Kriminalität» sich immer wieder den übergrossen Strukturen der international agierenden, organisierten Kriminalität gegenübersehen. Auch beim Dezernat Digitale Kriminalität beginnt die Arbeit mit dem Suchen und Sichern von Spuren. Wie ist ein Hacker in ein System eingedrungen? Wie hat er sich darin bewegt? Ist ein Modus Operandi erkennbar? Die Arbeit beginnt lokal, geht aber schnell über die Landesgrenzen hinaus. «Mit Kantönligeist kommt man hier nicht weit», sagt Sutter.

Denn auch das ist Teil von Sutters Arbeit. Dabei unterscheidet sich der Job von Andreas Sutter in mehreren Punkten von dem seiner Kolleginnen und Kollegen bei der Basler Staatsanwaltschaft. Seine Täter kriegt er selten selber zu fassen: Wenn eine internationale Hackergruppe – wie zuletzt beim Erziehungsdepartement geschehen – in ein Netzwerk eindringt, Daten abzieht und dann versucht, Geld damit zu erpressen, müssen sich diese kaum je vor dem Basler Strafgericht verantworten. In seinen bisherigen Jahren hat Sutter noch nie als Staatsanwalt eine Anklageschrift formulieren müssen. Stattdessen hilft er bei der Aufklärung von Fällen rund um die Welt. «Es ist wichtig, zu zeigen, dass die Strafverfolgung aktiv ist. Und der Erfolg ist ja durchaus vorhanden, nur halt nicht in Basel selber.»

Gesetze lassen sich nur bedingt auf digitale Welt anpassen

Ein weiterer Unterschied: Delikte wie Mord und Totschlag funktionieren gleich, seit Kain Abel den Schädel eingeschlagen hat. Hier ändern allenfalls die Ermittlungsmöglichkeiten oder manchmal auch der rechtliche Rahmen. Sutter dagegen muss sich mit Straftaten auseinandersetzen, für die es keine Blaupause gibt. Und man muss vorwegnehmen können, wie Cyberverbrechen in ein paar Jahren aussehen könnten.

Ein fiktives Beispiel: Jemand eröffnet einen Schuhladen im Metaverse, also in der virtuellen Welt. Im Gegensatz zu einem Onlineshop verkauft man dort keine Schuhe, die ein paar Tage später per Post geliefert werden, son-

Erziehungsdepartement ist noch immer am Aufräumen

Datendiebstahl Der bekannteste Fall von Cyberkriminalität in Basel ereignete sich vermutlich in den vergangenen Weihnachtsferien. Unbekannte drangen in den Bildungsserver edubs des Erziehungsdepartements ein und kopierten 1,2 Terabyte Daten von insgesamt 761 Lehr- und Fachpersonen, Schülerinnen und Schülern und Verwaltungsangestellten. Rund einen Monat später drohten die Hacker mit der Veröffentlichung der teils sensiblen Daten im Darknet, was dann im Mai auch geschah.

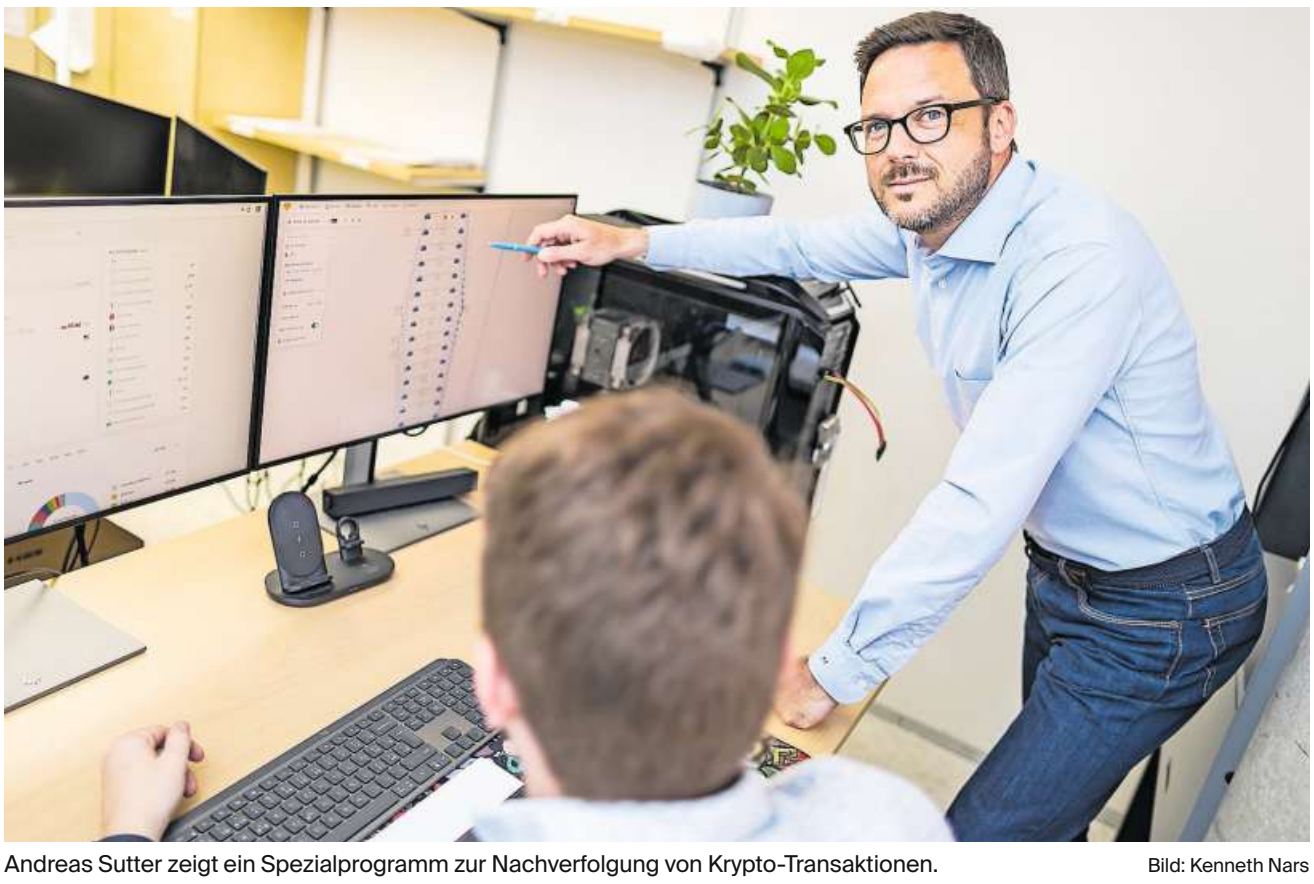
Seither sind vier Personen aus der IT-Abteilung des Erziehungsdepartements mit der Aufarbeitung beschäftigt. Denn die Zahl der indirekt Betroffenen, etwa wenn die Elternliste einer Schulklasse veröffentlicht wurde, ist um ein Vielfaches höher. Als Folge des Hackerangriffs seien die Sicherheitsvorkehrungen im Erziehungsdepartement erhöht worden, sagte der zuständige Regierungsrat Conradin Cramer kürzlich im Parlament. Ein externes Security Operation Center, also ein Team von Fachpersonen, welche die Sicherheit analysieren, werde in Betrieb genommen und die Erneuerung der Systeminfrastruktur beschleunigt.

> «Es ist wichtig zu zeigen, dass die Strafverfolgung aktiv ist. Und der Erfolg ist ja da, nur halt nicht in Basel selber.»
>
> **Andreas Sutter**
> Staatsanwalt

mittlerweile mit einem hoch spezialisierten Team im digitalen Raum. Bild: Getty

dern nur digitale Treter, die dann ein digitales Alter Ego – der sogenannte Avatar – in der virtuellen Welt tragen kann. So weit, so kompliziert. Wenn es nun aber jemand schafft, sich der digitalen Schuhe zu behändigen, fangen die rechtlichen Fragen erst an: Denn ein Diebstahl liegt gemäss dem Schweizerischen Strafgesetzbuch nur vor, wenn jemand eine fremde, bewegliche Sache einer anderen Person zur Aneignung wegnimmt. «Die Delikte, mit denen wir zu tun haben, lassen sich teilweise schwierig auf die Gesetzestexte ummünzen», sagt Sutter.

Auch die digitalen Währungen stellten die Ermittler vor Probleme: Was passiert mit Kryptowährungen, wenn die Staatsanwaltschaft sie sicherstellt? Im Gegensatz zu Bargeld oder traditionellen Bankkonten musste zuerst eine Bank gefunden werden, wo die digitalen Vermögenswerte aufbewahrt werden konnten. Solche Fragen dürften in Zukunft auch in der Öffentlichkeit reihenweise auftauchen, denn virtuelle Welten wie das Metaverse stecken noch in Kinderschuhen. «Grundsätzlich dürfte dort alles, was es in der analogen Welt gibt, ebenfalls passieren – von Sexualdelikten bis zu Drogenhandel», sagt Sutter. «Wir sind aber bei vielen Entwicklungen noch am Anfang.»



Andreas Sutter zeigt ein Spezialprogramm zur Nachverfolgung von Krypto-Transaktionen. Bild: Kenneth Nars