Stories – Wie ist es und wie könnte es sein?

Fall 1 – Der Bankangestellte

Ist-Situation

Die StA Wien bekommt Anfang 2017 eine Anzeige einer Bank, dass der Bankangestellte A verschiedene Kredite in Höhe von insgesamt 2 Millionen Euro an fünf Kunden vergab. Die Namen der Kunden werden aufgrund des Bankgeheimnisses vorerst nicht genannt und über eine Kontenregisterabfrage ermittelt. A verweigert die Aussage, die Kunden werden als Zeugen befragt. Die Staatsanwaltschaft vollzieht daraufhin mit dem LKA Wien Hausdurchsuchungen in der Wohnung von A, wobei zahlreiche Datenträger sichergestellt wurden: USB-Sticks, Images von Festplatten sowie ein verschlüsseltes Mobiltelefon). Die forensisch gesicherte Rohdatenmenge beträgt 2,5 TB.

Die Techniker des LKA Wien bereiten die Datenmenge nach Absprache mit den Ermittlern innerhalb 6 Monaten auf und filtern aus dem relevanten Datenbestand 160 GB heraus, der aus Mails (PST-Dateien), Office-Dokumenten und einem Truecrypt-Container mit einer relativ schwachen Verschlüsselung besteht. Der Staatsanwaltschaft wird mitgeteilt, dass man kein Suchprogramm hat, woraufhin über das Bundeskriminalamt die Daten in eine Suchsoftware eingespielt werden. Die verschlüsselten Daten können laut LKA nicht entschlüsselt werden und werden nicht eingespielt. Die Suchsoftware indiziert die Daten binnen einem Monat. Über die Suchsoftware stellt sich heraus, dass es sich bei den Kreditnehmern um Bekannte von B handelt, daher könnte es sich um Mittäter handeln. Die Staatsanwaltschaft beantragt daraufhin die Öffnung der Konten der Kunden bei Gericht. Da die Kontounterlagen von der Bank in unterschiedlichen Formaten (Excel, PDF, Papier) herausgegeben werden, müssen sie großteils manuell ausgewertet werden. Es stellt erst nach mehreren Wochen heraus, dass das Geld unmittelbar nach Auszahlung des Kredits in bar behoben wurden.

Es folgen weitere Hausdurchsuchungen Anfang 2018 in den Wohnungen der Kreditnehmer, wobei ein Teil des Bargelds und weitere Datenträger mit insgesamt 4 TB sichergestellt werden. Auch hier gelingt eine Reduktion nach Filterung auf 1 TB. Dieser Datenbestand wird in den bisherigen Datenbestand in

der Suchsoftware hinzugefügt. Bis die Daten in der Suchsoftware zur Verfügung stehen vergehen wieder 2 Monate. In den Wohnungen wurden zusätzlich mehrere Kisten mit Papierzetteln sichergestellt, die händisch gesichtet werden, der scheinbar relevante Teil davon nach drei Monaten vollständig digitalisiert wird (5 GB), und in Folge ebenfalls in die Suchsoftware eingespielt werden.

Nach mehreren Monaten kann aus den Daten ermittelt werden, dass zahlreiche Rechnungen mit hohen Beträgen mit Bargeld bezahlt wurden. Einer der Mittäter von A hat laut einem Kontoeröffnungsvertrag ein Konto bei einer Bank in Frankreich. Aufgrund eines Rechtshilfeersuchens ergibt sich, dass ein hoher Bargeldbetrag ca. zeitgleich mit der Bargeldbehebung am österreichischen Konto eingezahlt wurde. Nach weiterer Recherche ergibt sich, dass der Mittäter zu dieser Zeit einen Flug nach Frankreich gebucht hat. Das noch am Konto befindliche Geld in Frankreich wird beschlagnahmt. Nach Abzug der Rechnungsbeträge, des sichergestellten Teils des Bargelds und des am Konto in Frankreich sichergestellten Geldbetrags kann der Rest in Höhe von 1,4 Millionen Euro nicht mehr aufgefunden werden, die Täter schweigen dazu eisern.

Anfang 2019 werden A und seine Mittäter angeklagt, das LKA Wien übergibt nun die Daten auf Festplatten dem Gericht, die die Festplatten in der Verwahrstelle verwahrt. Während der Hauptverhandlung stellt A den Beweisantrag, dass man in den Daten danach suchen möge, dass er eigentlich per Mail von den Mittätern mit dem Umbringen seiner Frau bedroht wurde und nur aus Todesangst das Geld auszahlte. Der Richter weist den Antrag von A ab und die Mittäter werden Mitte 2019 verurteilt. Der oberste Gerichtshof hebt das Urteil auf und trägt dem Gericht auf, den Beweis wie beantragt aufzunehmen. Der Richter ordnet Anfang 2020 in der Hauptverhandlung die Beweisaufnahme an und weist das LKA Wien an, die Festplatten wieder in Suchsoftware einspielen. Durch die Lagerung in der Verwahrstelle sind sie unlesbar geworden. Mangels Überprüfungsmöglichkeit der Daten, folgt im Zweifel ein Freispruch für A.

Soll-Situation:

Die StA Wien bekommt Anfang 2017 eine Anzeige einer Bank, dass der Bankangestellte A verschiedene Kredite in Höhe von insgesamt 2 Millionen Euro an fünf Kunden vergab. Die Namen der Kunden werden aufgrund des Bankgeheimnisses vorerst nicht genannt und über eine Kontenregisterabfrage ermittelt. A verweigert die Aussage, die Kunden werden als Zeugen befragt. Die Staatsanwaltschaft vollzieht daraufhin mit dem LKA Wien Hausdurchsuchungen in der Wohnung von A, wobei zahlreiche Datenträger sichergestellt wurden: USB-Sticks, Images von Festplatten sowie ein verschlüsseltes Mobiltelefon). Die forensisch gesicherte Rohdatenmenge beträgt 2,5 TB.

Die **ausreichend ausgestatteten** Techniker des LKA Wien bereiten die Datenmenge nach Absprache mit den **Ermittlern innerhalb 3 Monaten** auf und filtern aus dem relevanten Datenbestand 160 GB

heraus, der aus Mails (PST-Dateien), Office-Dokumenten und einem Truecrypt-Container mit einer relativ schwachen Verschlüsselung besteht**. Der Staatsanwalt ordnet nach Rücksprache mit dem LKA Wien an, die Daten in einem zentralen Rechenzentrum mit Analysesoftware auszuwerten.** Die verschlüsselten Daten können laut LKA nicht entschlüsselt werden, wobei die IT-Experten der WKStA im Rechenzentrum mit selbst installierten Programmen noch einen Versuch starten. Analysesoftware indiziert die Daten im Rechenzentrum binnen zwei Wochen. Es stellt sich sehr rasch heraus, dass es sich bei den Kreditnehmern um Bekannte von B handelt, daher könnte es sich um Mittäter handeln. Die Staatsanwaltschaft beantragt daraufhin die Öffnung der Konten der Kunden bei Gericht. Da die Kontounterlagen von der Bank **elektronisch, die Transaktionen in strukturierten Formaten** herausgegeben werden müsse, werden die digitalen Daten am Server gespeichert. **Die Staatsanwaltschaft übermittelt die Daten auch an das Rechenzentrum und die Daten werden in Analysesoftware eingespielt. Es stellt sich binnen Tagen heraus, dass das Geld unmittelbar nach Auszahlung des Kredits in bar behoben wurden. Währenddessen haben die IT-Experten den True-Crypt Container geknackt, da ein Täter ein Passwort in seinem Mail-Account genannt hat. Darin befinden sich Bankschließfachverträge, die (mangels gesetzlicher Grundlage nicht im österreichischen Kontenregister enthalten sind) und daher bisher unbekannt waren. Die Staatsanwaltschaft findet dort 1 Million Euro Bargeld, das sie sicherstellt.**

Es folgen Ende 2017 weitere Hausdurchsuchungen in den Wohnungen der Kreditnehmer, wobei ein Teil des Bargelds und weitere Datenträger mit insgesamt 4 TB sichergestellt werden. Auch hier gelingt eine Reduktion nach Filterung auf 1 TB. Dieser Analysedatenausgangsbestand wird in den bisherigen Datenbestand zu Analysesoftware hinzugefügt. In den Wohnungen wurden zusätzlich mehrere Kisten mit Papierzetteln sichergestellt, die durch **Nutzung einer Scanstraße** vollständig digitalisiert werden (15 GB) und in Folge ebenfalls in Analysesoftware eingespielt werden. **Nach zwei Wochen** kann aus den Daten ermittelt werden, dass zahlreiche Rechnungen mit hohen Beträgen mit Bargeld bezahlt wurden. Einer der Mittäter von A hat laut einem Kontoeröffnungsvertrag ein Konto bei einer Bank in Frankreich. Aufgrund eines Rechtshilfeersuchens ergibt sich, dass ein hoher Bargeldbetrag ca. zeitgleich mit der Bargeldbehebung am österreichischen Konto eingezahlt wurde. **Nach weiterer Recherche ergibt sich quasi sofort, dass der Mittäter zu dieser Zeit einen Flug nach Frankreich gebucht hat, da Analysesoftware automatisiert Buchungen von Flügen in E-Mails erkennt und diese vermutlichen Aufenthaltsorte graphisch darstellt.**

Weil alle Unterlagen - und nicht nur der scheinbar relevante Teil - digitalisiert wurden, erkennt die Analysesoftware anhand eines Dokuments, auf dem nur eine Kontonummer enthalten ist, und einer Notiz auf einem anderen Dokument, dass sie einem Täter zuzuordnen ist. Es können auf diesem Konto 100.000 Euro beschlagnahmt werden.

Mitte 2018 werden A und seine Mittäter angeklagt, **das Gericht erhält durch Freischaltung den Zugriff auf das Rechenzentrum.** Während der Hauptverhandlung stellt A den Beweisantrag, dass man in den Daten danach suchen möge, dass er eigentlich von den Mittätern bedroht wurde und nur aus Todesangst das Geld auszahlte. **Der Richter beauftragt das LKA Wien den Beweis wie beantragt zu erheben, wobei mit Analysesoftware binnen 1 Woche berichtet wird, dass man die angebliche Drohung nicht findet.** A und die Mittäter werden verurteilt, das Urteil wird rechtskräftig. **Die Daten aus dem Rechenzentrum werden archiviert.**

Unterschiede:

Aktueller Stand	**Rechenzentrum mit Analysesoftware**
Verfahrensdauer: 3 Jahre, weil • Mühsame Gewinnung des Überblicks über unbekannte Datenmenge • Teil des Tathergangs trotz großem Zeitaufwand unaufgeklärt • Datenhandling verursacht Probleme und Zeitverlust	Verfahrensdauer: 1,5 Jahre, weil • Raschere Gewinnung von Ermittlungsansätzen • Schnellere Aufklärung des Tathergangs • Friktionslose Datenübergabe (zwischen Kripo , StA und Gericht
Ausgang: Freispruch für A wegen Datenverlust, Schuldsprüche für Mittäter	Ausgang: Schuldsprüche für alle
Sichergestellte Vermögenswerte: Geld am Konto + Teil des Bargelds	Sichergestellte Vermögenswerte: Zusätzlich 1,5 Millionen Euro

Fall 2: Der Leistungsträger, der Treuhänder und die Untreue

Ist-Situation

Bei der WKStA wird Anfang 2016 folgende Anzeige erstattet: Die X-GmbH besitzt mehrere Liegenschaften. Der Rechtsanwalt Mag. A ist als deren Alleingesellschaftergeschäftsführer im Firmenbuch eingetragen. Im Jahr 2014 soll die Y-GmbH an die X-GmbH eine Liegenschaft im Wert von 20 Millionen Euro um einen weit zu niedrigen Kaufpreis, nämlich um 10 Millionen Euro, verkauft haben, wodurch der Y-GmbH ein Schaden von 10 Millionen Euro entstanden sei. Der Geschäftsführer der mittlerweile insolventen Y-GmbH war damals Dr. B. Tatsächlich war das Grundstück damals mindestens 20 Millionen wert.

Die WKStA vernimmt Dr. B, der angibt, dass er ein Gutachten bei Diplomingenieur C in Auftrag gegeben hat, das einen Marktpreis von 10 Millionen Euro ausgewiesen hat. Über das Firmenbuch geht hervor, dass Dr. B in einem Firmengeflecht von zehn Firmen - mit zahlreichen ineinander verwobenen Beteiligungen - Gesellschafter ist. In einer dieser Gesellschaften ist der Rechtsanwalt Mag. A ebenfalls Gesellschafter. Der Masseverwalter der Y-GmbH wird nach Beischaffung des Insolvenzakts um Auskunft über den Geschäftsfall ersucht wird. Der Masseverwalter übergibt eine Kopie eines Ordners mit der Aufschrift „Verkauf der Liegenschaft an die Y-GmbH“. Der Ordner wird digitalisiert und bei der WKStA am Server gespeichert (bzw. digitalisiert) und durchgesehen. Dabei fällt auf, dass Dr. B offensichtlich stark darauf drängte die Liegenschaft zu verkaufen.

Der Masseverwalter teilt der WKStA zusätzlich schriftlich mit, dass sich Dr. B. von 2012 bis 2015 stark überhöhte Geschäftsführerbezüge auszahlen ließ und einen Porsche im Wert von 80.000 Euro als Firmen-PKW ankaufte, an den sich aber weder die Sekretärin, noch die anderen zehn Mitarbeiter erinnern können, ihn je am Firmengelände gesehen zu haben.

Die WKStA bestellt Mitte 2016 einen Immobiliensachverständigen um den Wert der Liegenschaft zu ermitteln und das hinzugezogene Bundeskriminalamt stellt bei der Y-GmbH durch Anfertigung von forensischen Kopien den Datenbestand des von Dr. B. genutzten Laptops sicher, die Buchhaltung der Jahre 2012 bis 2016 wird elektronisch gesichert und es wird ein Image des Mailservers (Exchange) erstellt. Vom File-Server werden Teile des Rechnungswesens (gescannte Rechnungen, Verträge, etc.) und die Ordner der maßgeblichen Personen gesichert. In einer Schublade werden zehn nicht bezeichnete USB-Sticks gefunden. Der Laptop von Dr. B. ist verschlüsselt und kann vorerst nicht ausgewertet werden. Die Buchhaltung wurde in einem sehr seltenen Buchhaltungsprogramm geführt (z.B. Masonic) und die Datenbankdateien gesichert. Der ebenfalls für die Krida-Delikte bestellte Buchsachverständige teilt mit, dass die Datenbankdateien nicht ohne aufwändige Aufbereitung

ausgewertet werden können, weil die Datenbankdateien nicht in den Buchhaltungs(analyse)programmen ACL und BMD in dieser Form eingelesen werden können. Da mittlerweile der Masseverwalter den Server durch Verkauf verwertet hat, ist es nicht mehr möglich die Buchhaltung nochmals „besser“ sicherzustellen, weshalb man einen IT-Dienstleister beauftragt, die schon gesicherten Buchhaltungsdateien in lesbare Form zu bringen. Dies wird 6 Monate dauern und ca. 20.000 Euro kosten. Die Mails, der Inhalt der USB-Sticks und die Dateien vom File-Server werden in Suchsoftware eingespielt.

Aufgrund Recherchen in den Mails und dem File-Server wird Anfang 2017 erhoben, dass Dr. B. scheinbar etliche Privataufwendungen (Pkw, Flugreisen) an die Y-GmbH verrechnet hat. Daraufhin erfolgt eine Hausdurchsuchung bei Dr. B, bei der dessen Stand-PC und ein iPad sichergestellt werden (500 GB Rohdaten). Unter Pizzaschachteln im Kleiderschrank findet man neben einigen Zeitschriften mit Yachten auch Urlaubsfotos von Dr. B, auf dem auch DI C zu sehen sind. Sowohl Dr. B. als auch C verweigern die Aussage. Das BKA findet auf dem Stand-PC Kinderpornos und die WKStA scheidet dieses Verfahren an die StA Wien aus. Das BKA übergibt eine Kopie der Festplatte mit diesen Daten an das LKA Wien (- die Auswertung wird bis Ende 2019 andauern).

Ebenfalls Anfang 2017 wird das Gutachten des Immobiliensachverständigen fertiggestellt: Die Liegenschaft war tatsächlich mindestens 20 Millionen Euro wert. Mag. A steht im Verdacht, dass er mit Dr. B beim Verkauf der Liegenschaft um 10 Millionen Euro zusammengewirkt hat.

Ende 2017 legt der Gutachter, der nunmehr die aufbereitete Buchhaltung auswerten konnte, sein Gutachten vor, in dem er diverse Kridadelikte aufarbeitete. Parallel ermittelte das Bundeskriminalamt bereits hinsichtlich entsprechender Vorsätze. Eine Anklage gegen Dr. B. als Geschäftsführer der Y-GmbH wird Anfang 2018 hinsichtlich dieser Vorwürfe bei Gericht eingebracht. Dr. B. wird Ende 2018 wegen dieser Vorwürfe verurteilt.

Ende 2019 zeigt sich aufgrund eines Suchauftrags aus dem Datenbestand, dass Mag. A zahlreiche Geschäfte mit Dr. B machte und dieser tatsächlich der Treugeber der X-GmbH war, somit Dr. B die Liegenschaft de facto unterpreisig an sich selbst verkaufte. Nach einigen Kontenöffnung ist Mitte 2020 ersichtlich, dass DI C für sein falsches Gutachten 500.000 Euro nach Legung einer Scheinrechnung aus einer der Unternehmen aus dem Firmengeflecht des Dr. B erhalten hat.

Dr. B, Mag. A und DI C werden wegen dieses Faktums Ende 2020 wegen Untreue und betrügerischer Krida angeklagt und Ende 2021 verurteilt.

Soll-Situation

Bei der WKStA wird Anfang 2016 folgende Anzeige erstattet: Die X-GmbH besitzt mehrere Liegenschaften. Der Rechtsanwalt Mag. A ist als deren Alleingesellschaftergeschäftsführer im Firmenbuch eingetragen. Im Jahr 2014 soll die Y-GmbH an die X-GmbH eine Liegenschaft im Wert von 20 Millionen Euro um einen weit zu niedrigen Kaufpreis, nämlich um 10 Millionen Euro, verkauft haben, wodurch der Y-GmbH ein Schaden von 10 Millionen Euro entstanden sei. Der Geschäftsführer der mittlerweile insolventen Y-GmbH war damals Dr. B. Tatsächlich war das Grundstück damals mindestens 20 Millionen wert.

Die WKStA vernimmt Dr. B, der angibt, dass er ein Gutachten bei Diplomingenieur C in Auftrag gegeben hat, das einen Marktpreis von 10 Millionen Euro ausgewiesen hat, und legt dieses vor. Über das Firmenbuch geht hervor, dass Dr. B in einem Firmengeflecht von zehn Firmen mit zahlreichen ineinander verwobenen Beteiligungen Gesellschafter ist. In einer dieser Gesellschaften ist der Rechtsanwalt Mag. A ebenfalls Gesellschafter. Der Masseverwalter der Y-GmbH wird nach Beischaffung des Insolvenzakts um Auskunft über den Geschäftsfall ersucht wird. Der Masseverwalter übergibt eine Kopie eines Ordners mit der Aufschrift „Verkauf der Liegenschaft an die Y-GmbH“. Der Ordner wird digitalisiert und bei der WKStA am Server gespeichert (bzw. digitalisiert) und durchgesehen. Dabei fällt auf, dass Dr. B offensichtlich stark darauf drängte die Liegenschaft zu verkaufen.

Der Masseverwalter teilt der WKStA zusätzlich schriftlich mit, dass sich Dr. B. von 2012 bis 2015 stark überhöhte Geschäftsführerbezüge auszahlen ließ und einen Porsche im Wert von 80.000 Euro als Firmen-PKW ankaufte, an den sich aber weder sie Sekretärin, noch die anderen zehn Mitarbeiter erinnern konnten, ihn gesehen zu haben.

Die WKStA bestellt Mitte 2016 einen Immobiliensachverständigen um den Wert der Liegenschaft zu ermitteln und das hinzugezogene Bundeskriminalamt stellt bei der Y-GmbH durch Anfertigung von forensischen Kopien den Datenbestand des von Dr. B. genutzten Laptops sicher, die Buchhaltung der Jahre 2012 bis 2016 wird elektronisch gesichert und es wird ein Image des Mailservers (Exchange) erstellt. Vom File-Server werden Teile des Rechnungswesens (gescannte Rechnungen, Verträge, etc.) und die Ordner der maßgeblichen Personen gesichert. In einer Schublade werden zehn nicht bezeichnete USB-Sticks gefunden. Der Laptop von Dr. B. ist verschlüsselt und kann vorerst nicht ausgewertet werden. **Die Buchhaltung wurde unter Beiziehung von IT-Experten fachgerecht über eine Exportfunktion gesichert und kann nachfolgend im Rechenzentrum mit wenig Aufwand eingespielt werden. Die Wirtschaftsexperten der WKStA können aus der Buchhaltung die Zahlungsflüsse in wenigen Wochen nachvollziehen. Für die Feststellung der Zahlungsunfähigkeit wird ein Buchsachverständiger bestellt, der Zugriff auf die Daten im Rechenzentrum hat. Die Mails, der Inhalt der USB-Sticks und die Dateien vom File-Server werden im Rechenzentrum in die**

Analysesoftware eingespielt. Aufgrund Recherchen in den Mails und dem File-Server wird innerhalb weniger Wochen erhoben, dass Dr. B. scheinbar etliche Privataufwendungen (Pkw, Flugreisen) an die Y-GmbH verrechnet hat, da die Rechnungen in Analysesoftware automatisch erkannt werden. Weitere Rechnungen von zwei verschiedenen ausländischen Unternehmen in Höhe von 1 Million Euro für Beratungsleistungen aus dem Jahr 2014 werden von Analysesoftware erkannt, wobei über die Analysesoftware auch erkannt wird, dass tatsächlich auf den Rechnungen eine Kontonummer der Z-GmbH, eine der Gesellschaften aus dem Firmengeflecht von Dr. B, enthalten ist. Die Wirtschaftsexperten stellen fest, dass die Zahlungen verbucht wurden.

Daraufhin erfolgt noch im Herbst 2016 eine Hausdurchsuchung bei Dr. B und der Z-GmbH. Bei Dr. B wird dessen Stand-PC und ein iPad sichergestellt (500 GB Rohdaten). Unter Pizzaschachteln im Kleiderschrank findet man neben einigen Zeitschriften mit Yachten auch Urlaubsfotos von Dr. B, auf dem auch DI C zu sehen sind. Sowohl Dr. B. als auch C verweigern die Aussage. Das BKA findet auf dem Stand-PC Kinderpornos und die WKStA scheidet dieses Verfahren an die StA Wien aus. **Das BKA erteilt dem LKA Wien Zugriff auf die (Teil-)Daten im Rechenzentrum für die entsprechenden Ermittlungen (die bereits Anfang 2017 nach Abgleich mit Hashwerten von bekannter Kinderpornographie abgeschlossen werden). Der Firmenserver der Z-GmbH wird ebenfalls sichergestellt (1 TB) und in das Rechenzentrum komplett zu Analysesoftware übertragen. Die auch hier „richtig" sichergestellte Buchhaltung und die sichergestellten Daten werden ausgewertet und Anfang 2017 festgestellt, dass es keine Beratungsleistungen gab, somit eine Untreue begangen wurde. Weil die Zahlungen aber als Aufwand verbucht wurde und in den Steuererklärungen der Y-GmbH und damit der Gewinn in der Steuererklärung für das Jahr 2014 um 1 Million Euro zu niedrig dargestellt und 250.000 Euro zu wenig Unternehmenssteuern abgeführt wurde, leitet die WKStA zusätzlich ein Verfahren nach dem Finanzstrafgesetz wegen Abgabenhinterziehung und Abgabenbetrug ein. Die Steuerfahndung erhält dafür Zugriff auf den Datenbestand im Rechenzentrum.**

Ebenfalls Anfang 2017 werden die Gutachten des Immobiliensachverständigen und des Buchsachverständigen fertiggestellt: Die Liegenschaft war tatsächlich mindestens 20 Millionen Euro wert, die Y-GmbH war bereits 2014 zahlungsunfähig. **Die Steuerfahndung erkennt währenddessen, dass weitere falsche Steuererklärungen (Umsatzsteuererklärung) abgegeben wurden. Unter dem Druck der zahlreichen Vorwürfe legt Dr. B ein umfangreiches Geständnis (mit Ausnahme hinsichtlich des Liegenschaftsverkaufs) ab.** Eine Anklage gegen Dr. B wird Mitte 2017 bei Gericht hinsichtlich der Untreuevorwürfe (mit Ausnahme jener des Liegenschaftsverkaufs), Kridavorwürfe und jenen nach dem **Finanzstrafgesetz** wird eingebracht, auch die **StA Wien klagt Dr. B. wegen Kinderpornographie an.** Dr. B. wird noch Ende 2017 wegen der bisher angeklagten Vorwürfe aufgrund seines Geständnisses rechtskräftig verurteilt werden.

Noch im Herbst 2018 zeigt sich aus dem Datenbestand in Analysesoftware, dass Mag. A zahlreiche Geschäfte mit Dr. B machte und dieser der Treugeber der X-GmbH war, somit Dr. B die Liegenschaft de facto an sich selbst verkaufte. **Mehrere Entwürfe des Gutachtens werden in den Daten nach entsprechender „Modellierung" (daher wie die Analysesoftware Gutachten als solche erkennen kann) gefunden, wobei DI C ursprünglich ein richtiges Gutachten erstattet haben dürfte, jedoch auf Drängen von Dr. B. und unter Einbindung von Mag. AG nach jedem überarbeiteten Entwurf der Preis bis schließlich auf 10 Millionen Euro niedriger wurde. DI C legt angesichts dieser Beweise ebenfalls ein Geständnis ab. Er gibt zu, dass er für sein falsches Gutachten 500.000 Euro nach Legung einer Scheinrechnung aus einer der Unternehmen aus dem Firmengeflecht des Dr. B erhalten hat.** Mag. A gibt nun ebenfalls zu, dass er ein Strohmann von Dr. B war und er Beitragstäter von Dr. B war, der sich in Wahrheit die Liegenschaft selber zugeschanzt hat. Dr. B, Mag. A und DI C werden Anfang 2019 wegen Untreue angeklagt und im Herbst 2019 rechtskräftig verurteilt.

Unterschiede:

Aktueller Stand	**Rechenzentrum mit Analysesoftware**
Verfahrensdauer: 5 Jahre, weil • Sicherstellung und Auswertung der Buchhaltung mangelhaft (+ Kosten für SV) • Auswertung von Kinderpornographie nicht abgeschlossen;	Verfahrensdauer: 3,5 Jahre, weil • Sicherstellung und sofort Beginn der Auswertung der Buchhaltung (keine Kosten für SV) • Auswertung von Kinderpornographie sehr rasch und führt durch Belastung zum Geständnis und zum schnelleren Erfolg
• Ausgang: Abgabenhinterziehung und Untreuefaktum nicht entdeckt;	• Ausgang: Abgabenhinterziehung und Untreuefaktum entdeckt; Faktum Liegenschaftsverkauf durch Beweis der Absprache zwischen Dr. B. und DI C weiter abgesichert • Steuerfahndung für Finanzdelikte und LKA Wien für Kinderpornographie auf Knopfdruck Zugriff gewährt.

Fall 3: Business as usual

Ist-Situation

Die WKStA erhält Anfang 2017 eine Whistle-Blowing-Meldung eines Mitarbeiters eines Baukonzerns, wonach bei einem großen Bauprojekt 2013 an einen Bürgermeister für die Baubewilligung eine Bestechungszahlung von 300.000 Euro geleistet worden sein soll. Aufgrund der glaubwürdigen Darstellung leitet die WKStA Ermittlungen ein und vernimmt sowohl den Bürgermeister als auch die verantwortlichen Personen im Baukonzern. Alle streiten die Vorwürfe vehement ab. Der Whistle-Blower macht eine weitere Meldung und fügt dieses Mal ein weitgehend geschwärztes und eingescanntes E-Mail an. Im Mail wird ein Konto mit der Bemerkung angeführt, dass „alles erledigt und nun Zahltag" sei. Eine Abfrage im Kontenregister ergibt, dass das Konto der Ehegattin des Bürgermeisters zugeordnet ist. Es erfolgt noch vor Sommer 2017 eine Hausdurchsuchung im Amt der Stadtgemeinde und im Baukonzern. In der Stadtgemeinde werden Akten und der Mailserver gesichert und die Papierunterlagen digitalisiert (ca. 300 GB). Im Baukonzern, der über einen sehr alten Firmenserver, einem eigenen Intranet (mit relevanten Dokumenten) und selbstprogrammierter Software zur Dokumentation von Bauprojekten verfügt, gestaltet sich die Sicherstellung vorerst unkompliziert, da der dortige IT-Administrator auf Weisung des Vorstands die relevanten Daten herausgibt (30 GB). Im Büro eines Vorstands findet man einen USB-Stick im Mistkübel, der mitgenommen wird. Sämtliche Daten werden beim Bundesamt für Korruptionsbekämpfung (BAK) in Suchsoftware eingespielt. Auf dem USB-Stick findet man Mitte 2017 eine Excel-Liste in der 50 Bauprojekte und daneben Geldbeträge festgehalten sind. Eines der Bauprojekte ist jene mit der Bewilligung des Bürgermeisters und in der Excel-Liste steht „300T". Die Ermittler gehen nun davon aus, dass diese Liste Bestechungszahlungen für die jeweiligen Bauprojekte enthält, wodurch sich das Verfahren zu einem der größten bisherigen Strafverfahren entwickeln wird.

Es werden im Herbst 2017 in den 30 Stadtgemeinden, deren Bürgermeister bzw. Abteilungen die 50 Baubewilligungen erteilt haben, gleichzeitig Hausdurchsuchungen durchgeführt und jeweils Stand-PCs, Server, Mails und physische Ordner sichergestellt (insgesamt 15 TB). Zeitgleich findet beim Baukonzern eine weitere Hausdurchsuchung statt, wobei dieses Mal die Geschäftsführung jede Kooperation verweigert. Mithilfe der Mitarbeiter werden aus den bereits dargestellten Systemen insgesamt 40 TB zu den Bauprojekten sichergestellt. Die Sicherung dauert mehrere Wochen und Ende 2017 werden die Daten auf NAS-Geräten vom BAK abgeholt. Aufgrund der zahlreichen Bauprojekte und Verdächtigen werden dutzende Beschuldigtenvernehmungen durchgeführt. Der Akt hat innerhalb kürzester Zeit fast 1000 Ordnungsnummern. Zahlreiche Stellungnahmen samt digitalen Urkundenvorlagen werden an die WKStA geschickt, die dem BAK vor Durchführung der Vernehmungen übermittelt werden müssen.

Mangels eines gemeinsamen „Shares“ werden fast jede Woche digitale Aktenkopien des Ermittlungsakts der WKStA vom BAK auf DVD persönlich abgeholt. Da noch keine ausreichenden Kapazitäten für die Auswertung der sichergestellten Datenmenge vorhanden sind, werden die Daten erst nach einer Ausschreibung für die notwendige Hardware und deren Beschaffung Mitte 2018 mit Suchsoftware durchsuchbar gemacht. WKStA und BAK müssen aufgrund des Umfangs der Ermittlungen eine Prioritätensetzung bei den einzelnen Fakten vollziehen. Bis Mitte 2019 können die ersten zehn Fakten ausermittelt werden. Die Ermittler wissen, dass hohe Bargeldbeträge auf den Konten der Beamten eingezahlt wurden, die sie teilweise nicht erklären können. Wie man die Behebungen getarnt hat, ist aber bis zuletzt nicht klar. Die Ende 2019 eingebrachten Anklagen führen bis Mitte 2020 teils zu Schuld-, teils im Zweifel zu Freisprüchen, weil einige Angeklagte für die Bareinzahlungen nicht widerlegbare Rechtfertigungen behaupten.

Bei der Auswertung der Daten fiel auf, dass es zu „rauschenden Privatfesten“ in der Geschäftsführungsetage gekommen sein dürfte, die der Baukonzern bezahlte. Da das BAK bereits personell mit den „Hauptfakten“ ausgelastet ist, wird die Bearbeitung dieser Untreuefakten vom Bundeskriminalamt übernommen. Das BAK berechtigt das BKA auf die Daten in Suchsoftware zuzugreifen. Aufgrund der Ermittlungen des Bundeskriminalamts kommt hervor, dass auch der Leiter des zuständigen Magistrats für Bauwesen bei einer der Feiern war und für diverse Veranstaltungen Eintrittskarten (Salzburger Festspiele, VIP-Karten, etc.) erhielt. Es folgen bis 2021 weitere Anklagen gegen die Verantwortlichen des Baukonzerns und der Gemeinden sowie gegen den zuständigen im Magistrat für Bauwesen, wobei es immer wieder Frei- und Schuldsprüche gibt, je nachdem ob Bargeldzuflüsse glaubhaft erklärt werden können oder nicht.

Soll-Situation:

Die WKStA erhält Anfang 2017 eine Whistle-Blowing Meldung eines Mitarbeiters eines Baukonzerns, wonach bei einem großen Bauprojekt 2013 an einen Bürgermeister für die Baubewilligung eine Bestechungszahlung von 300.000 Euro geleistet worden sein soll. Aufgrund der glaubwürdigen Darstellung leitet die WKStA Ermittlungen ein und vernimmt sowohl den Bürgermeister als auch die verantwortlichen Personen im Baukonzern. Alle streiten die Vorwürfe vehement ab. Der Whistle-Blower macht eine weitere Meldung und fügt dieses Mal ein weitgehend geschwärztes und eingescanntes E-Mail an. Im Mail wird ein Konto genannt mit der Bemerkung, dass „alles erledigt und nun Zahltag“ sei. Eine Abfrage im Kontenregister ergibt, dass das Konto der Ehegattin des Bürgermeisters zugeordnet ist. Es erfolgt noch vor Sommer 2017 eine Hausdurchsuchung im Amt der Stadtgemeinde und im Baukonzern. In der Stadtgemeinde werden Akten und der Mailserver gesichert und jene auf Papier digitalisiert (ca. 300 GB). Im Baukonzern, der über einen sehr alten Firmenserve, einem eigenen Intranet (mit relevanten Dokumenten) und selbstprogrammierter Software zur

Dokumentation von Bauprojekten verfügt, gestaltet sich die Sicherstellung vorerst unkompliziert, da der dortige IT-Administrator die relevanten Daten herausgibt (30 GB). Im Büro eines Vorstands findet man einen USB-Stick im Mistkübel, der mitgenommen wird. **Sämtliche Daten werden im Rechenzentrum in Analysesoftware eingespielt.** Auf dem USB-Stick findet man Mitte 2017 eine Excel-Liste in der 50 Bauprojekte und daneben Geldbeträge festgehalten sind. Eines der Bauprojekte ist jene mit der Bewilligung des Bürgermeisters und in der Excel-Liste steht daneben „300T". Die Ermittler gehen nun davon aus, dass diese Liste Bestechungszahlungen in anderen Bereichen enthält, wodurch sich das Verfahren zu einem der größten Strafverfahren entwickeln wird.

Es werden im Herbst 2017 in den 30 Stadtgemeinden, deren Bürgermeister bzw. Abteilungen die 50 Baubewilligungen erteilt haben, gleichzeitig Hausdurchsuchungen durchgeführt und jeweils Stand-PCs, Server, Mails und physische Ordner sichergestellt (insgesamt 15 TB). Zeitgleich findet beim Baukonzern eine weitere Hausdurchsuchung statt, wobei dieses Mal die Geschäftsführung jede Kooperation verweigert. Mithilfe der Mitarbeiter werden aus den bereits dargestellten Systemen insgesamt 40 TB zu den Bauprojekten sichergestellt. Die Sicherung dauert mehrere Wochen und Ende 2017 werden die Daten auf NAS-Geräten vom BAK abgeholt. Aufgrund der zahlreichen Bauprojekte und Verdächtigen werden dutzende Beschuldigtenvernehmungen durchgeführt. Der Akt hat innerhalb kürzester Zeit fast 1000 Ordnungsnummern. Zahlreiche Stellungnahmen samt digitalen Urkundenvorlagen werden an die WKStA geschickt, die dem BAK vor Durchführung der Vernehmungen übermittelt werden müssen. **Das BAK greift über das Rechenzentrum auf eine stets aktuelle Kopie des Ermittlungsakts der WKStA zu. Da im Rechenzentrum in kürzester Zeit entsprechende Ressourcen bereitgestellt werden können, können bereits Anfang 2018 die ersten Teildatenmengen in Analysesoftware eingespielt werden.** WKStA und BAK müssen aufgrund des Umfangs der Ermittlungen eine Prioritätensetzung bei den einzelnen Fakten vollziehen. **Bis Mitte 2018 können die ersten zehn Fakten ausermittelt werden, da die Analysesoftware sehr rasch das Kommunikationsgeflecht offenlegt. Sie erkennt, dass bei allen Baustellen (auch) Rechnungen von fünf Subunternehmern gestellt wurden, deren Rechnungsbetrag genau den Beträgen in der Excel-Liste entsprechen. Nach Abgleich mit der Dokumentation der Bauprojekte geht hervor, dass die genannten Rechnungen offenbar grundlos oder doch weit überhöht gestellt wurden. In Folge werden Ende 2018 Hausdurchsuchungen bei den fünf Subunternehmern durchgeführt und wiederum E-Mails, der File-Server und die Buchhaltung sichergestellt (7 TB). Nach Einspielen im Rechenzentrum und Integration in den Analysesoftware Datenbestand ergibt sich Mitte 2019, dass die fünf Subunternehmer bei den betreffenden Rechnungen keine oder nur sehr geringe (Arbeits-)Leistungen dokumentiert haben. Das überwiesene Geld des Baukonzern wurde in Tranchen bar behoben, die auffallend mit den Bargeldeinzahlungen auf den Konten der Beamten korrelieren. Durch Aufdeckung dieses Betrugsmusters können die restlichen Fakten bereits bis Ende 2019 weitgehend aufgeklärt werden.**

Anfang 2020 werden die Anklagen eingebracht. Aufgrund der Aufdeckung des Geldflusses über die Subunternehmer folgen fast ausnahmslos Schuldsprüche gegen die Verantwortlichen des Baukonzerns, die Subunternehmer (als Beitragstäter) und die Beamten, zumal sich aufgrund der Dynamik viele Beschuldigte geständig zeigen.

Parallel fällt bis Mitte 2018 bei der Auswertung der Daten außerdem auf, dass es zu „rauschenden Privatfesten" in der Geschäftsführungsetage gekommen sein dürfte, die der Baukonzern bezahlte. Da das BAK bereits mit den „Hauptfakten" völlig ausgelastet ist, wird die Bearbeitung dieser Untreuefakten vom Bundeskriminalamt übernommen. **Das BAK berechtigt auch Ermittler des BKA auf die Daten im Rechenzentrum zuzugreifen.** Aufgrund der Ermittlungen des Bundeskriminalamts kommt hervor, dass auch der Leiter des zuständigen Magistrats für Bauwesen bei einer der Feiern war und für diverse Veranstaltungen Eintrittskarten (Festspiele, VIP-Karten, etc.) erhielt. Es folgen bis Ende 2019 Anklagen gegen die Verantwortlichen des Baukonzerns und der Gemeinden sowie gegen den zuständigen im Magistrat für Bauwesen.

Unterschiede:

Aktueller Stand	**Rechenzentrum mit Analysesoftware**
Verfahrensdauer: 4 Jahre, weil • Betrugsmuster nicht vollständig erkannt wurde • Datentransfer zwischen Kripo und StA umständlich • IT-Ressourcen erst zur Verfügung gestellt werden mussten;	Verfahrensdauer: 2,5 Jahre, weil • Sehr rasch Betrugsmuster vollständig erkannt wurde und Folgemaßnahmen zielgerichtet möglich; • Datenübermittlung (Stellungnahmen) „auf Knopfdruck" möglich; • IT-Ressourcen nach Bedarf erweiterbar ohne Zeitverlust;
• Ausgang: o Teils Frei- und Schuldsprüche, weil Verantwortung nicht widerlegbar; o Subunternehmer nicht als Täter erkannt;	• Ausgang: o Fast nur Schuldsprüche, weil Geldfluss kaum mehr widerlegbar; o Subunternehmer als Täter erkannt;