



DEUTSCHE INKERMAN FRAUD WEEKLY

Ausgabe 172

Die Fraud Weekly gibt einen wöchentlichen Überblick über eine Auswahl von Betrugs- und Korruptionsfällen, die von unserem Corporate Intelligence & Investigations Team zusammengestellt und analysiert werden.

Inhalt

Im Zuge sich ausweitender Korruptionsermittlung verhaftet die brasilianische Polizei zwei Personen

Cyber-Experten warnen vor Gefahren im Zusammenhang mit Hacking durch Drohnen

Kurznachrichten

Brexit-Referendum schafft optimale Betrugsbedingungen

Kontaktieren Sie uns

IM ZUGE SICH AUSWEITENDER KORRUPTIONSERMITTLUNG VERHAFTET DIE BRASILIANISCHE POLIZEI ZWEI PERSONEN

Eigenen Angaben zufolge hat die Polizei in Brasilien am 2. August 2016 zwei Personen festgenommen und mehrere Häuser durchsucht. Grund war eine Ausweitung der Petrobras-Ermittlung wegen Verdacht auf mutmaßliche Korruption bei der Baufirma Queiroz Galvao. Die übergeordnete Polizeiaktion, Operation Lava Jato genannt, begann vor zwei Jahren und hat bereits zu mehreren Verurteilungen wegen Bestechung und Geldwäsche geführt. Im Zuge der derzeitigen Ermittlungen wird Vorwürfen nachgegangen, dass ein Kartell von Baufirmen Angebote für Aufträge von Petrobras manipuliert und dem Unternehmen zu hohe Beträge in Rechnung gestellt hat. Anschließend soll das zusätzliche Geld dazu benutzt worden sein, Führungskräfte von Petrobras zu bestechen und Wahlkampagnen von Politikern zu finanzieren. Zu den Inhaftierten zählen Ildelfonso Colares Filho, der ehemalige Präsident der Baufirma, und Othon Zanoide Moraes Filho, der Ex-Direktor der Öl- und Gasdivision. Ihnen wird vorgeworfen, sie hätten versucht, die Ermittlungen zu behindern. Darüber hinaus sagte die Staatsanwaltschaft, es gebe Beweise dafür, dass „Queiroz Galvao ein Kartell mit anderen Baufirmen gebildet hat, das aktiv an den Anpassungen beteiligt war [...] wobei zahlreiche Dokumente die Aussagen von mindestens fünf Mitarbeitern bestätigten.“ Im November 2014 waren die Beschuldigten schon einmal wegen Vorwürfen von Korruption, Betrug und Geldwäsche festgenommen worden. Ein Richter ließ sie jedoch fünf Tage später wieder frei, weil er der Ansicht war, dass weitere Ermittlungen nötig seien, um eine Inhaftierung zu rechtfertigen.

Die **Trustworthy Accountability Group** hat die ersten **100 Teilnehmer** bekannt gegeben, die sich ihrem **Register von Unternehmen** angeschlossen haben, das sich dem Ziel verschrieben hat, die **Integrität des digitalen Werbungs-Ökosystems zu schützen**.

POSITIVE/NEGATIVE HIGHLIGHTS DER LETZTEN WOCHE

	Unaoil SAM (unabhängige Untersuchung durch Petrofac findet keine Beweise zur Stützung von Bestechungsvorwürfen); 38 Studios (nach vierjähriger Betrugsermittlung wird keine Strafanzeige gegen das ehemalige Games-Unternehmen erhoben)
	Yahoo! (Zugangsdaten von 200 Millionen Nutzern angeblich gehackt und im Dark Web zum Verkauf angeboten); Richard Hotchin (nach Ermittlung der britischen Steuerbehörde HMRC erhält Geschäftsmann aus Lincoln Haftstrafe von 21 Monaten wegen Steuerbetrug)

Bei 75 % der führenden 20 US-amerikanischen Handelsbanken wurde Malware gefunden.

CYBER-EXPERTEN WARNEN VOR GEFAHREN IM ZUSAMMENHANG MIT HACKING DURCH DROHNEN

Internet-Sicherheitsforscher haben gewarnt, dass Drohnen für Cyberangriffe eingesetzt werden könnten.

Die Experten äußerten diese Bedenken im Vorfeld der Black Hat Konferenz, die in dieser Woche in Las Vegas stattfindet.

WLAN, Bluetooth-Geräte und kontaktlose Zahlungskarten seien,

KURZNACHRICHTEN

Ein Vorhaben, Millionen öffentlicher Datensätze zu löschen, könnte Untersuchungen von schweren Betrugs-, Geldwäsche- und Korruptionsdelikten erschweren. Die britische Regierungsbehörde Companies House, die Einzelheiten über alle in GB registrierten Firmen speichert, diskutiert Vorschläge, alle Daten von Firmen zu löschen, die vor mehr als sechs Jahren ihre Geschäfte eingestellt haben. Derzeit werden Daten zu aufgelösten Firmen 20 Jahre lang aufbewahrt. Sollte die Maßnahme gebilligt werden, würden auch die

festgenommenen 38-jährigen Komplizen erwarten Anklagen wegen Hacking, Verschwörung und Beschaffung von Geld durch Vorspiegelung falscher Tatsachen.

Drei ehemalige Banker aus Irland wurden für ihren Anteil am Kollaps der Anglo Irish Bank während der Finanzkrise von 2008 zu insgesamt acht Jahren Haft verurteilt. Willie McAteer, John Bowe und Denis Casey wurden der Verschwörung zur Vertuschung von Verlusten von Milliarden von Euros für schuldig befunden, womit sie zum Finanz-Crash des Landes beitrugen. Nach

so die Experten, gleichermaßen gefährdet. Potenzielle Angriffe wemöglichen so, Daten aus Privatwohnungen sowie aus öffentlichen Gebäuden oder Einkaufszentren leicht abzufangen.

Da Drohnen sehr nah an Geräte herankommen, würde es ihnen leicht sein, auch WLAN- und Bluetooth-Geräte mit geringer Reichweite (z. B. Tastaturen) zu kompromittieren.

Möglichkeiten von Banken, Anwaltskanzleien und Kreditagenturen vollständiger Due-Diligence-Prüfungen durchzuführen, erheblich eingeschränkt werden.

In einer Aktion von Interpol und der nigerianischen Kommission für Wirtschafts- und Finanzkriminalität (EFCC) wurde der mutmaßliche Anführer eines internationalen kriminellen Netzwerks festgenommen. Der nur „Mike“ genannte nigerianische Staatsbürger soll ein Netzwerk von 40 Personen geleitet haben, das über längere Zeit Cyberangriffe und Malware-Injektionen gegen E-Mail-Konten von Unternehmen in aller Welt durchgeführt hat, v.a. in Australien, Südafrika und den USA. Den Verdächtigen und einen ebenfalls

dem Betrug wurde die Bank 2009 verstaatlicht und dann allmählich aufgelöst. Bisher sind nur relativ wenige Banker für ihre Rolle in der Finanzkrise zur Rechenschaft gezogen und strafrechtlich verfolgt worden.

Ein ehemaliger UBS-Händler, der 2012 wegen Beteiligung an einem Betrug in Höhe von 1,4 Mrd. GBP ins Gefängnis musste, hat davor gewarnt, dass trotz harten Vorgehens gegen die Branche ähnliche Betrügereien wieder passieren könnten. Kweku Adoboli sagte in dieser Woche in einem Interview, der Druck auf seine früheren Kollegen, Profite zu machen, sei so hoch wie eh und je, weshalb es auch weiterhin zu fiktiven Transaktionen kommen werde.

BREXIT-REFERENDUM SCHAFFT OPTIMALE BETRUGSBEDINGUNGEN

Nach der „Brexit“-Entscheidung Großbritanniens nutzen Betrüger die Verwundbarkeit und Verwirrung der Menschen bezüglich der Zukunft des Landes zu ihren Gunsten aus. Die Brexit-Entscheidung hat ein „perfektes Ökosystem“ für Betrug entstehen lassen, obwohl insgesamt die durch Betrug verursachten Schäden in den letzten sechs Monaten gesunken sind. Die aus Betrugsfällen resultierenden Kosten sanken in der ersten Jahreshälfte auf 328 Mio. GBP, gegenüber 385 Mio. GBP im selben Zeitraum des Vorjahrs, waren also um 57 Mio. GBP (14%) geringer. Nichtsdestotrotz hat die britische Entscheidung, die Europäische Union zu verlassen, ein Umfeld von Unsicherheit und wirtschaftlicher Volatilität geschaffen, das sich Kriminelle zunutze machen können. In einem diesbezüglichen Bericht wurde ein aktueller Fall erwähnt, bei dem sich ein Betrüger als ein milliardenschwerer Banker des Papstes ausgab, um eine Reederei um 73 Mio. GBP zu betrügen. Der vorgebliche Banker überlistete sie, indem er behauptete, für Geldanlagen unter Benützung einer geheimen päpstlichen Handelsplattform eine Rendite von 1.200% erreichen zu können. Einige schwere Betrugsfälle, die in diesem Jahr aufgezeichnet wurden, gingen sogar soweit, dass es den Tätern gelang, ihre Unternehmensopfer dazu zu verleiten, ihnen große Summen zu überlassen, die die Operationsfähigkeit der Unternehmen wesentlich beeinträchtigten.



SCHÜTZEN SIE IHRE MARKE UND IHRE REPUTATION

Der **Total Intelligence Platform Service (TIPs)** der Inkerman Group ist ein einzigartiges fortschrittliches Informationssystem, das den elektronischen Horizont absucht, um Bedrohungen und Trends zu ermitteln und Ihrem Unternehmen frühzeitig Warnhinweise zu geben. Unsere Online-Informationsdashboards liefern Ihnen 24/7 umfassende, dynamische und maßgeschneiderte Informationen.

Wissen - Gewissheit - Einsichten - umfassend - Trendanalysen

Für weitere Auskünfte kontaktieren Sie bitte das Corporate Intelligence Team der Inkerman Group.

KONTAKTIEREN SIE UNS

Für weitere Informationen zu diesen Themen sowie dazu, wie die Deutsche Inkerman GmbH Sie unterstützen kann, kontaktieren Sie uns noch heute unter:

info@deutscheinkerman.de - + 49 (0) 2132 968 5151 - www.deutscheinkerman.de

Deutsche Inkerman GmbH - Am Meerkamp 17-19 - 40667 - Meerbusch (Düsseldorf) - DEUTSCHLAND

The Inkerman Group - Operations Centre - Inkerman House - 3-4 Elwick Road - Ashford - Kent - TN23 1PF - ENGLAND

The Inkerman Group - 1 Cornhill - London - EC3V 3ND - ENGLAND

[Klicken Sie hier](#) um von der Verteilerliste gelöscht zu werden.