Neue Betrugsmasche: Erster Fake President Fall mit Stimmimitation durch KI-Software

- Erster Fake President Schadensfall durch künstliche Intelligenz mit Stimmimitations-Software
- Tochterunternehmen im Ausland besonders gefährdet
- Fake President Schadensfälle auf gleichbleibend hohem Niveau, Schadenssummen steigen seit Jahren
- Laut FBI allein 2018 von über 20.000 Fälle mit weltweiten Schäden in Höhe von insgesamt 1,2 Milliarden (Mrd.) US-Dollar (USD)
- Weitere Varianten der Betrugsmasche: Fake IT Security Mitarbeiter, Geschenkkarten, Besteller- und Zahlungsbetrug

Hamburg, 4. September 2019 – Der falsche Chef wird künstlich intelligent: Erstmals kam bei der sogenannten „Fake President" Betrugsmasche, auch als „CEO Fraud", „Chef-Betrug" oder „Chefmasche" bekannt, eine Stimmimitations-Software zum Einsatz. Diese Software basiert auf „Machine Learning": Mithilfe eines selbstlernenden Algorithmus' kann sie innerhalb von einigen Minuten die Stimme eines Menschen erlernen und anschließend nachahmen – inklusive der individuellen Sprachmelodie oder dem landestypischen Akzent. Damit hat die bisher meist allein auf E-Mails basierende Betrugsmasche eine neue Variante. Trotz des relativ hohen Bekanntheitsgrads der Betrugsmasche bewegen sich die Fallzahlen seit Jahren auf relativ gleichbleibend hohem Niveau. Die Schadenssummen haben in den letzten Jahren allerdings deutlich zugenommen.

„Der falsche Johannes": Wenn der falsche Chef die richtige Stimme hat

„Die Täter gehen immer gewiefter vor. Mit der erstmaligen Nutzung von künstlicher Intelligenz bei der Fake President Betrugsmasche erreichen wir eine neue Evolutionsstufe", sagt Ron van het Hof, CEO von Euler Hermes in Deutschland, Österreich und der Schweiz. „Das ist aber erst der Anfang: Software zur Stimm- oder Handschriftenimitation oder auch Deepfake-Videos eröffnen Betrügern in Zukunft noch viele neue Möglichkeiten. In einem oder zwei Jahren gibt es vielleicht den ersten Fake President Fall, bei dem die Zahlungsanweisung per Deepfake-Video per Whatsapp kam."

Inzwischen sind viele dieser Anwendungen bereits relativ weit entwickelt, dass sie insbesondere am Telefon vom „Original" nur schwer zu unterscheiden sind. So auch beim Anruf des vermeintlichen deutschen CEO eines Energieunternehmens beim Chef der britischen Niederlassung.

„Bei uns heißt dieser Schadensfall ‚Der falsche Johannes': Der falsche Chef hat die richtige Stimme", sagt Rüdiger Kirsch, Betrugsexperte bei Euler Hermes. „Konkret gab der CEO bei diesem Fall der dem Chef des britischen Tochterunternehmens nicht nur per E-Mails, sondern vorab auch telefonisch Zahlungsanweisungen. Dieser hat sich zwar etwas gewundert, da er jedoch die Stimme eindeutig erkannte, hat er den Auftrag trotzdem durchgeführt. Er hat 220.000 Euro (EUR) auf ein Konto in Ungarn überwiesen. Das gesamte Geld war weg."

Die Begründung des falschen Chefs: Er habe den Transaktionszeitraum der Bank am Freitagnachmittag verpasst. Die Überweisung hätte vor 16 Uhr getätigt werden müssen, damit die Zahlung noch vor dem Wochenende erfolgen kann. Durch die Zeitverschiebung sei die Überweisung deshalb nur noch durch die britische Tochter möglich – denn in Großbritannien war es erst 15 Uhr.

Stimmimitations-Software aktuell nur auf Englisch: ausländische Niederlassungen gefährdet

„Es ist kein Zufall, dass es ausgerechnet eine britische Tochter des Unternehmens war, die Ziel des Betrugs wurde", sagt Kirsch. „Die Zeitverschiebung ist dafür zwar nicht ausschlaggebend, sondern vielmehr die Tatsache, dass die vermutlich verwendete Stimmimitations-Software aktuell nur Englisch kann. Unternehmen sollten daher ihre ausländischen Niederlassungen besonders sensibilisieren, dass die Betrüger ihre Masche weiterentwickelt haben."

Der britische Chef war grundsätzlich mit dem Fake-President-Betrug vertraut, das Unternehmen hatte seine Auslandstöchter alle davor gewarnt. Durch die eindeutige Zuordnung der Stimme schrillten die Alarmglocken allerdings nicht laut genug. Misstrauisch wurde er erst, als die versprochene unternehmensinterne Zahlung auf sich warten ließ – und er eine weitere Zahlung veranlassen sollte.

Gier provoziert Fehler: Zweite Überweisung wird vereitelt
„Der Täter wurde nach seinem ersten Erfolg gierig und witterte das große Geld“, sagt Kirsch. „Dabei wurde er auch schlampiger und machte einige Fehler: Sein zweiter Anruf kam von einer österreichischen statt einer deutschen Nummer.“

Auch die Begründung war widersprüchlich: Der ungarische Lieferant bestehe darauf, dass die Zahlung vom gleichen Konto käme, begründete der falsche Chef die zweite Zahlung. Das Empfängerkonto war allerdings ein gänzlich anderes als beim ersten Mal. Erst da wurde der Brite stutzig und rief den echten CEO an: „Kurios war dann, dass der falsche Johannes anrief, während er mit dem echten am Telefon war“, sagt Kirsch.

Die neue Variante kombiniert die bisherige E-Mail Kommunikation mit Telefonanrufen. Die Anrufe dienten insbesondere zur Vertrauensbildung und waren maßgeblicher Erfolgsfaktor. Die Zahlungsanweisungen mit den mehrstelligen Kontodaten kamen – wie in der allgemeinen Geschäftspraxis – per E-Mail. Gut für die britische Tochter, denn die Telefonate des falschen Chefs wurden nicht aufgezeichnet. Durch die E-Mails mit den Zahlungsanweisungen und Kontodaten war der Tathergang und Schaden jedoch eindeutig nachweisbar.“

Fallzahlen weiterhin auf hohem Niveau – Schadenssummen steigen weiter
Seit 2014 tritt die Fake President Betrugsmasche in Deutschland vermehrt auf und nahm in den folgenden Jahren stark zu. Der im April 2019 vom Federal Bureau of Investigation (FBI) veröffentlichte Internet Crime Report geht 2018 von über 20.000 Fake-President-Opfern aus. Laut der Studie haben die Täter haben mit der Betrugsmasche im vergangenen Jahr weltweit insgesamt 1,2 Milliarden (Mrd.) US-Dollar (USD) erbeutet – das ist der größte finanzielle Posten in der Rubrik Schäden durch Internet-Kriminalität. Zwischen 2013 und 2018 haben sich die bekannten weltweiten Schäden durch Fake President auf insgesamt 12,5 Mrd. USD summiert – und die Dunkelziffer ist weiterhin hoch.

Euler Hermes: 65 Fälle mit einem Schadenvolumen von insgesamt mehr als 165 Mio. EUR
„Trotz gestiegenem Bewusstsein, dass es solche Betrugsmaschen gibt, sehen wir bisher ebenfalls keinen wirklichen Rückgang der Fallzahlen – und die Schadenshöhen steigen weiterhin an“, sagt Kirsch. „In den letzten vier Jahren haben wir allein bei Euler Hermes etwa 65 Fälle mit einem gemeldeten Schadenvolumen von mehr als 165 Millionen (Mio.) EUR verzeichnet. Anfangs waren es noch Einzelfälle, inzwischen sind es durchschnittlich etwa 20 Fälle pro Jahr.“

Alle Branchen und Unternehmensgrößen betroffen, Schadenshöhe variiert
Die Schadenshöhe der Opfer variiert dabei zwischen rund 150.000 EUR und 50 Millionen – mit Tendenz nach oben. In Sicherheit fühlen kann sich dabei keine Branche:

„Bei den betroffenen Unternehmen waren praktisch alle Branchen und Unternehmensgrößen vertreten, zunehmend auch kleine und mittelständische Unternehmen – überdurchschnittlich oft Unternehmen mit Tochtergesellschaften im Ausland“, sagt Kirsch. „Kommt es zu einer Überweisung ist Zeit Geld: Die ersten 36 bis maximal 72 Stunden sind entscheidend, ob vielleicht noch ein Teil des Geldes durch schnelles Handeln und einen guten Draht zur Hausbank zurückgeholt werden kann.“

Nur etwa 1 Mio. EUR konnten bei den 65 Fällen durch schnelles Handeln und den Rückruf der Überweisungen über die Hausbank wieder beschafft werden. In den meisten Fällen war das Geld weg. Die Spur verlor sich auf Konten in China, Hongkong, Afrika, Russland, Israel oder Osteuropa. Auch Ermittlungserfolge sind selten und Täter konnten bisher nur in wenigen Einzelfällen gefasst werden.

Neue Varianten: Von Stimmimitation über Fake IT bis zu Besteller- und Zahlungsbetrug
„Die Täter werden immer professioneller“, sagt Kirsch. „Laufend entwickeln sie ihre Methoden weiter. Erst kamen Zahlungs- und Bestellerbetrug, Fake IT Mitarbeiter und schließlich Geschenkkarten. Dass sie jetzt auf künstliche Intelligenz zurückgreifen ist nur logisch. Das werden wir in Zukunft sicher häufig sehen. Wenn sie gut gemacht sind, ist das ein enormes Risiko und es könnte Fallzahlen und Schadenssummen nach oben treiben.“

Evolutionsstufen Fake President Betrug

Evolutionsstufe	Vorgehen
Frühstadium: E-Mail	E-Mail mit z.T. Schreib- und/oder Grammatikfehler, schlecht getarnter Absender, abweichende E-Mail Adresse: Max Mustermann [max@12345.com]
Evolutionsstufe 1: Social Engineering	Korrekte Rechtschreibung, gut getarnte Absender mit z.B. fehlende Buchstaben, Buchstaben- oder Zahlendrehern: Max Mustermann [max.mustermann@musterman.com] Social Engineering – durch Wertschätzung des Mitarbeiters/in und insbesondere durch hohen Druck des falschen externen Anwalts, z.T. müssen die Mitarbeiter alle 1-2 Stunden ihre Vertraulichkeitsvereinbarung erneuern
Evolutionsstufe 2: Gehacktes Intranet	Korrekte, gehackte/gedoppelte Absenderadresse: Max Mustermann [max.mustermann@mustermann.com] Betrüger hacken sich ins Intranet und verweilen dort für einige Tage, spionieren Zuständigkeiten und Gepflogenheiten aus wie z.B. Umgangston, E-Mail Stil (Du/Sie, förmlich/informell), Ansprechpartner Social Engineering durch Interna verbessert – Wissen um interne Informationen schafft Vertrauen
Evolutionsstufe 3: Telefonanruf	Gezieltes Social Engineering: Betrüger ruft eine Mitarbeiterin in der Buchhaltung an, um ihr zum 10-jährigen Firmenjubiläum zu gratulieren. Wenige Wochen später ruft er für den Fake President Betrug erneut an – sie erkennt seine Stimme und führt gemäß der Aufforderung per E-Mail die Überweisungen aus.
Evolutionsstufe 4: Fake IT Security Mitarbeiter	Gezieltes Social Engineering: Kurz nach der E-Mail mit der gefälschten Zahlungsaufforderung ruft ein Fake IT Mitarbeiter in der Buchhaltung an, um dem Mitarbeiter mitzuteilen, dass bei ihm ein Fake President Versuch entdeckt worden sei. Alles sei unter Kontrolle und der Mitarbeiter solle „zum Schein“ mitspielen, damit man die Betrüger auf frischer Tat ertappen könne. Es werde aber keine echte Zahlung ausgelöst, weil man mit der Hausbank kooperiere. Der Mitarbeiter überweist – Geld weg.
Evolutionsstufe 5: Stimmimitation	Aktueller Fall mit Stimmimitationssoftware: Software ahmt Sprachmelodie und Akzente nach, so dass der CEO nach dieser telefonischen Bestätigung denkt, die Anweisung per E-Mail käme tatsächlich vom echten Konzern-Chef.
Mögliche zukünftige Evolutionsstufen: Deepfake, Video, Whatsapp	Mit weiterem Fortschritt bei Deepfake-Videos ist diese Technik als nächste Evolutionsstufe denkbar. Aktuell könnten zwar gefälschte Video-Nachrichten per Whatsapp etc. versendet werden, eine „Konversation“ per Video-Fake für Anweisungen des falschen CEO mit eventuellen Rückfragen des Buchhalters ist aktuell noch nicht verbreitet möglich.
Weitere „Untervarianten“	
Geschenkkarten, Besteller- und Zahlungsbetrug	Geschenkkarten: Mitarbeiter werden angewiesen werden, Geschenkkarten oder Gutscheine zu kaufen, für Jubiläumsfeiern oder ähnliche Anlässe Bestellerbetrug: Vortäuschung einer falschen Identität: Der Betrüger gibt sich als Kunde aus (oft als bestehender) bestellt Waren und lässt diese anschließend an eine abweichende Lieferadresse senden Zahlungsbetrug: Vortäuschung einer falschen Identität: Der Betrüger gibt sich für einen Lieferanten aus und gibt für die Bezahlung der bereits erfolgten Lieferung eine abweichende Kontoverbindung durch

Pressemeldung zum Anstieg der Schadensfälle bei Besteller- und Zahlungsbetrug:
https://www.eulerhermes.de/presse/besteller-und-zahlungsbetrug-auf-dem-vormarsch.html

CEO Blog Ron van het Hof zu „Social Engineering“ bei Fake President:
http://eulerhermes-blog.de/2019/06/fake-president-wie-betrueger-den-verstand-ausknipsen/

Die vollständige FBI-Studie „Internet Crime Report 2018“ finden Sie hier:
https://pdf.ic3.gov/2018_IC3Report.pdf

Pressekontakt:

Euler Hermes Deutschland (Hamburg)

Antje Wolters
Pressesprecherin
Telefon: +49 (0)40 8834-1033
Mobil: +49 (0)160 899 2772
antje.wolters@eulerhermes.com

Euler Hermes ist weltweiter Marktführer im Kreditversicherungsgeschäft und anerkannter Spezialist für Kaution und Garantien, Inkasso sowie Absicherung gegen Betrug oder politische Risiken. Das Unternehmen verfügt über mehr als 100 Jahre Erfahrung und bietet seinen Kunden umfassende Finanzdienstleistungen an, um sie im Liquiditäts- und Forderungsmanagement zu unterstützen.

Über das unternehmenseigene Monitoring-System verfolgt und analysiert Euler Hermes täglich die Insolvenzentwicklung von mehr als 40 Millionen kleiner, mittlerer und multinationaler Unternehmen. Insgesamt umfassen die Expertenanalysen Märkte, auf die 92% des globalen Bruttoinlandsprodukts (BIP) entfallen.

Mit dieser Expertise macht Euler Hermes den Welthandel sicherer und gibt den weltweit über 66.000 Kunden das notwendige Vertrauen in ihre Geschäfte und deren Bezahlung. Als Tochtergesellschaft der Allianz und mit einem AA-Rating von Standard & Poor’s ist Euler Hermes im Schadensfall der finanzstarke Partner an der Seite seiner Kunden.

Das Unternehmen mit Hauptsitz in Paris ist in über 50 Ländern vertreten und beschäftigt rund 5.800 Mitarbeiter weltweit. 2018 wies Euler Hermes einen konsolidierten Umsatz von EUR 2,7 Milliarden Euro aus und versicherte weltweit Geschäftstransaktionen im Wert von EUR 962 Milliarden.

Weitere Informationen auf www.eulerhermes.de

Social Media

CEO Blog Ron van het Hof
LinkedIn Euler Hermes Deutschland
XING Euler Hermes Deutschland
YouTube Euler Hermes Deutschland
Twitter @eulerhermes

Hinweis bezüglich zukunftsgerichteter Aussagen: Die in dieser Meldung enthaltenen Informationen können Aussagen über zukünftige Erwartungen und andere zukunftsgerichtete Aussagen enthalten, die auf aktuellen Einschätzungen und Annahmen der Geschäftsführung basieren, und bekannte und unbekannte Risiken sowie Unsicherheiten beinhalten, aufgrund derer die tatsächlichen Ergebnisse, Entwicklungen oder Ereignisse von den hier gemachten Aussagen wesentlich abweichen können. Neben zukunftsgerichteten Aussagen im jeweiligen Kontext spiegelt die Verwendung von Wörtern wie „kann“, „wird“, „sollte“, „erwartet“, „plant“, „beabsichtigt“, „glaubt“, „schätzt“, „prognostiziert“, „potenziell“ oder „weiterhin“ ebenfalls eine zukunftsgerichtete Aussage wider. Die tatsächlichen Ergebnisse, Entwicklungen oder Ereignisse können aufgrund verschiedener Faktoren von solchen zukunftsgerichteten Aussagen beträchtlich abweichen. Zu solchen Faktoren gehören u.a.: (i) die allgemeine konjunkturelle Lage einschließlich der branchenspezifischen Lage für das Kerngeschäft bzw. die Kernmärkte der Euler-Hermes-Gruppe, (ii) die Entwicklung der Finanzmärkte einschließlich der „Emerging Markets“ einschließlich Marktvolatilität, Liquidität und Kreditereignisse, (iii) die Häufigkeit und das Ausmaß der versicherten Schadenereignisse einschließlich solcher, die sich aus Naturkatastrophen ergeben; daneben auch die Schadenkostenentwicklung, (iv) Stornoraten, (v) Ausmaß der Kreditausfälle, (vi) Zinsniveau, (vii) Wechselkursentwicklungen einschließlich des Wechselkurses EUR-USD, (viii) Entwicklung der Wettbewerbsintensität, (ix) gesetzliche und aufsichtsrechtliche Änderungen einschließlich solcher bezüglich der Währungskonvergenz und der Europäischen Währungsunion, (x) Änderungen der Geldpolitik der Zentralbanken bzw. ausländischer Regierungen, (xi) Auswirkungen von Akquisitionen, einschließlich der damit verbundenen Integrationsthemen, (xii) Umstrukturierungsmaßnahmen, sowie (xiii) allgemeine Wettbewerbsfaktoren jeweils in einem örtlichen, regionalen, nationalen oder internationalen Rahmen. Die Eintrittswahrscheinlichkeit vieler dieser Faktoren kann durch Terroranschläge und deren Folgen noch weiter steigen. Das Unternehmen übernimmt keine Verpflichtung, zukunftsgerichtete Aussagen zu aktualisieren.