EULER HERMES

Fake President bekommt Konkurrenz: Besteller- und Zahlungsbetrug auf dem Vormarsch

- Schäden aus Täuschungsdelikten belaufen sich auf insgesamt über 190 Mio. EUR
- Bestellerbetrug: Fälle 2018 um 35% im Vergleich zum Vorjahr gestiegen
- Zahlungsbetrug: Fälle 2018 um 24% im Vergleich zum Vorjahr gestiegen
- „Massenware“: Betrugsmaschen sind wesentlich leichter durchzuführen als Fake President

Hamburg, 27. August 2019 – Der falsche Chef bekommt Konkurrenz. Neben der „Fake President“-Betrugsmasche sind in den letzten Jahren vor allem auch der Besteller- („Fake Identity“) und Zahlungsbetrug („Payment Diversion“) auf dem Vormarsch. Diese drei Täuschungsdelikte haben nach Analysen des weltweit führenden Kreditversicherers Euler Hermes bei vorwiegend deutschen Unternehmen sowie deren ausländischen Tochtergesellschaften seit 2014 zu Schäden von insgesamt über 190 Millionen Euro (Mio. EUR) geführt. Einen starken Anstieg bei den Fallzahlen gab es 2018 mit +35% im Vergleich zum Vorjahr vor allem beim Bestellerbetrug sowie mit +24% beim Zahlungsbetrug.

„Für Betrüger haben die beiden Betrugsmaschen Besteller- und Zahlungsbetrug durchaus ihren Reiz“, sagt Ron van het Hof, CEO von Euler Hermes in Deutschland, Österreich und der Schweiz. „Beide sind wesentlich einfacher durchzuführen als der Chef-Betrug.“

Ein Fake-President-Betrug erfordert relativ viel strategische Planung sowie eine zeitintensive Vorbereitung, beispielsweise zum Ausspähen der Gepflogenheiten. Zudem müssen die Täter fit sein im „Social Engineering“, um die Mitarbeiter dazu zu bringen, die gewünschten Zahlungen zu veranlassen und dies gleichzeitig geheim halten.

„Um Zahlungsströme umzuleiten oder eine abweichende Lieferadresse anzugeben, reicht in der Regel jedoch eine kurze E-Mail aus“, sagt Van het Hof. „Die Beträge sind zwar meist geringer, aber dafür geht es ratzfatz – sogar bei mehreren Firmen gleichzeitig. Die Zahlen sprechen hier Bände.“

Betrug wird meist erst bei Mahnlauf entdeckt: Täter und Beute längst über alle Berge

Beim Bestellerbetrug geben sich Hacker als Kunden aus. Sie lösen eine Bestellung aus und geben dann per E-Mail eine abweichende Lieferadresse für eine Bestellung an. So werden zum Beispiel Schuhe zu einem leerstehenden Gebäude geordert, die Rechnung geht an den bestehenden Kunden. Da dieser die Ware nie bestellt und vor allem auch nicht erhalten hat, bezahlt er die Rechnung nicht.

„Der Betrug kommt in der Regel erst mit dem Mahnlauf ans Licht – also je nach Zahlungsziel mehrere Wochen später. Bis dahin sind die Betrüger mit der Beute allerdings längst über alle Berge“, sagt Rüdiger Kirsch, Betrugsexperte bei Euler Hermes. „Die Fallzahlen sind bei beiden Täuschungsdelikten zuletzt stark gestiegen. Damit machen sie langsam aber sicher dem ‚großen Bruder‘ Fake President Konkurrenz.“

Hackerbetrug: ein Fall für die Vertrauensschadenversicherung

Die Ware oder das Geld sind weg und im schlimmsten Fall ist die Bilanz ruiniert – meist auch dann, wenn das Unternehmen eine Cyber- oder Warenkreditversicherung hat.

„Eine Warenkreditversicherung sichert gegen Zahlungsausfälle der Abnehmer – allerdings nur bei echten Unternehmen, wenn diese zum Beispiel insolvent sind. Auf einen Betrüger kann ich jedoch kein Versicherungslimit haben“, sagt Kirsch. „Wenn also ein Betrug zugrunde liegt und sich ein Hacker für ein Unternehmen ausgibt, die Ware an eine andere Adresse liefern lässt und dadurch ein finanzieller Schaden entsteht, ist dies kein Fall für die reguläre Warenkreditversicherung, sondern für eine Vertrauensschadenversicherung (VSV). Eine Cyberversicherung zahlt übrigens bei solchen Betrugsfällen durch Hacker meistens auch nicht.“

Cyberversicherungen beinhalten in der Regel schwerpunktmäßig Bausteine zum Schutz vor Haftpflichtrisiken sowie vor Schäden aus einer durch einen Cyberangriff entstandene Betriebsunterbrechung oder auch Schäden wegen fahrlässiger Falschbedienung. Umfangreiche Assistance-Dienstleistungen, bei Reputationsrisiken oder z.B. zur schnellen Wiederherstellung der IT-Infrastruktur oder des Webshops nach Cyberangriffen sind ebenfalls wichtige Elemente, zusammen

mit Bausteinen aus Rechtschutz- und D&O-Versicherung. Kriminelle Handlungen sind – wenn überhaupt – nur zu einem sehr kleinen Bruchteil abgedeckt.

Die Vertrauensschadenversicherung versichert hingegen primär gegen zielgerichtete, kriminelle Handlungen gegen ein Unternehmen. Unerlaubte Handlungen wie z.B. Betrug oder Veruntreuung durch die eigenen Mitarbeiter sowie durch externe Dritte – insbesondere Hacker – stehen bei der VSV im Vordergrund. Entsprechend sind finanzielle Schäden durch Fake President, Besteller- oder Zahlungsbetrug ebenso versichert wie Phishing, Keylogging oder „Man in the middle“ und „Man in the cloud“.

Übersicht Betrugsmaschen und jeweilige Vorgehensweise

Betrugsmasche	**Vorgehensweise**
Fake President / Chefbetrug	Vortäuschung einer falschen Identität: Der Betrüger gibt sich als CEO eines Unternehmens aus und veranlasst mittels „Social Engineering“ (z.B. durch besondere Wertschätzung sowie strenge Geheimhaltung und Druckausübung) Mitarbeiter (meist per E-Mail, z.T. auch telefonisch), Zahlungen zu tätigen, meist für als sehr dringend deklarierte, streng vertrauliche Unternehmenskäufe im Ausland
Fake Identity / 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
Payment Diversion / Zahlungsbetrug	Vortäuschung einer falschen Identität: Der Betrüger gibt sich für einen Lieferanten aus und gibt eine abweichende Kontoverbindung durch für die Bezahlung der bereits erfolgten Lieferung
Phishing	Der Betrüger versendet gefälschte E-Mails an Mitarbeiter eines Unternehmens zu reellen Themen. Ziel ist es, über den Link in der E-Mail Trojaner oder Keylogger einzuschleusen, um an sensible Unternehmensdaten zu gelangen
Keylogging	Der Betrüger schleust eine Software ins System ein, die Anmeldedaten und Passwörter aufzeichnet und speichert, z.B. von Kontodaten, Cloud-, Serverzugänge etc.
Man in the middle	Der Betrüger hackt sich in die Kommunikation zwischen zwei Kommunikationspartnern ein und besitzt so Zugriff auf den Datenverkehr. Er kann diese Daten einsehen und zu seinen Zwecken beliebig manipulieren
Man in the cloud	Der Betrüger hackt sich in eine Cloud, in der Unternehmensdaten ausgelagert sind (z.B. durch Keylogging) und kann diese Daten einsehen und beliebig manipulieren oder löschen bzw. Schadsoftware einschleusen

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/

PRESSEMITTEILUNG

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 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

(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.