Cybercrime profitiert von neuen Maschen, alten Fehlern und der Schwachstelle Mensch

- Cyberkriminalität: Schwerpunkte auf Ransomware- und „Social Engineering“-Delikten
- Zahlungsbetrug steigt 2020 um 35%, Bestellerbetrug um 25% im Vergleich zum Vorjahr; Entwicklung beim Anstieg schreibt sich 2021 bisher weiter fort
- „Hacking as a service“: Software und Schulungen im Darknet eröffnen Cyberkriminellen neue Einfallstore
- Deepfakes: Echtzeit-Konversationen in Video- und Audio-Calls technisch längst möglich
- Vorsicht Falle: Zunehmende Haftungsrisiken durch Cyberkriminalität

Hamburg, 11. November 2021 – Cybercrime wird immer arbeitsteiliger, internationaler und ist für die Täter oft hoch lukrativ. Homeoffice und mangelnde IT-Sicherheitsstandards spielen den Betrügern dabei ebenso in die Karten wie der technologische Fortschritt durch künstliche Intelligenz (KI). Cyberkriminelle setzen vor allem zwei Schwerpunkte: Ransomware-Delikte und Business-E-Mail-Compromise (BEC), zu denen auch Fake President (CEO Fraud), Zahlungsbetrug (Payment Diversion Fraud) und Bestellerbetrug (Fake Identity) gehören.

„Die immer professioneller werdenden Betrüger müssen heute nicht mal unbedingt selbst Hacker sein“, sagt Andreas Dondera, Cyberexperte beim Hamburger Landeskriminalamt. „In diesem Deliktsfeld bleibt die größte Schwachstelle aber der Mensch. Für Unternehmen ist es daher das A und O, ihre Mitarbeiter zu schulen und klare Regeln zu implementieren – etwa für den Umgang mit geänderten Kontodaten oder abweichenden Lieferadressen.“

Zahlungsbetrug bei Betrügern besonders beliebt: Fallzahlen steigen um 35%
Aktuelle Fälle gibt es in Hülle und Fülle. Erst kürzlich hat ein Unternehmen gleich zwei Mal eine Zahlung geleistet aufgrund einer Mail mit gefälschten Kontodaten – dadurch kam es zu einer Umlenkung des Zahlungsverkehrs und zu einem Schaden von insgesamt 1,3 Millionen Euro. Jüngst erbeuteten Betrüger sogar knapp 6 Mio. EUR durch eine manipulierte Rechnung. In den meisten Fällen liegen die Schadenssummen jedoch zwischen etwa 30.000 EUR und 1 Mio. EUR.

„Zahlungsbetrug ist aktuell auf dem Vormarsch“, sagt Rüdiger Kirsch, Betrugsexperte bei Euler Hermes. „Im letztem Jahr sind die Fallzahlen um 35% angestiegen, beim Bestellerbetrug waren es 25%. Das dürfte sich nach dem bisherigen Verlauf auch 2021 so fortsetzen. Das Homeoffice ist nicht nur wegen geringerer Sicherheitsstandards für die Betrüger ein wahres El Dorado. Es wird auch weniger kontrolliert und kommuniziert. Die Hürde, einen Kollegen anzurufen und ihn auf einen Vorgang anzusprechen, ist hier oft viel höher. Kontodaten werden da mal eben kurz geändert – oft mit fatalen Folgen. Kriminelle ‚Social Engineers‘ hacken nicht Systeme, sondern Menschen. Das Social Distancing spielt ihnen in die Karten.“

Homeoffice auf „Autopilot“ – Fake-President-Schaden in Höhe von 400.000 Euro
So auch bei einem Fake-President-Betrug, der sich vor Kurzem in Mitteldeutschland ereignete. Die Leiterin der Buchhaltung hinterfragt eine große Überweisungsaufforderung nicht, die sie im Homeoffice erreicht. Sie prüft nicht einmal die E-Mail-Adresse näher. Per Teams bittet sie eine Sachbearbeiterin im Homeoffice, die notwendige Zweitunterschrift zu leisten. So erhält die vom vermeintlichen CEO beauftragte Zahlung für angebliche Aktienkäufe über 400.000 Euro eine Freigabe.

In der Regel ist für den Erfolg beim CEO Fraud das "Social Engineering" entscheidend. Für diese Manipulation der Opfer ist eine Konversation in Echtzeit essenziell: Die Täter äußern Wertschätzung, zerstreuen Bedenken, bauen Druck auf oder beantworten Fragen – alles mit dem Ziel, das maximale Vertrauen in die Echtheit des Auftrags zu vermitteln.

Deepfakes: Echtzeit-Konversationen heben Social Engineering auf neue Ebene
„Die Betrüger gehen mit der Zeit: Manipulierte Audio- oder Video-Calls sind technisch längst möglich“, sagt Dirk Koch, selbständiger Rechtsanwalt und Cyberexperte. „Wenn der gefälschte CEO mit dem richtigen Aussehen und der richtigen Stimme Anweisungen für Überweisungen gibt, hebt das das Social Engineering und die Betrugsmöglichkeiten auf eine ganz neue Ebene. Auch die Tatsache, dass Hacker längt zu Dienstleistern geworden sind und ihre Software im Darknet zahlreichen Abnehmern zeitgleich anbieten, multipliziert die Risiken für Unternehmen.“

Bereits 2019 fiel der CEO der britischen Tochtergesellschaft eines deutschen Konzerns im Fall „Der falsche Johannes“ auf ein gefälschtes Stimmprofil herein, das sogar den leichten Akzent des deutschen Firmenchefs im Englischen imitierte. 220.000 Euro waren weg. 2020 erleichterten Betrüger mit einem Audio Deepfake eine Bank in Hongkong sogar um umgerechnet rund 30 Millionen Euro. Auch in Deutschland gab es vereinzelt Fälle, bei denen falsche Geschäftsführer mit gefälschten Stimmprofilen ihre Hausbank angerufen haben.

„In Frankreich haben Betrüger in einem Fall sogar ein ganzes Büro nachgebaut, um dem Video-Call die maximale Authentizität zu verleihen“, sagt Dondera. „Es überrascht mich, dass noch nicht mehr Kriminelle die technischen Möglichkeiten nutzen. Jedenfalls noch nicht.“

Plötzlich am Pranger: Cyberattacken bergen auch große Haftungsrisiken für Manager
Cyberkriminalität birgt neben finanziellen und datenschutzrechtlichen Risiken auch zunehmend Compliance- und Haftungsrisiken für Manager. Nicht umsonst steigen die Fälle, bei denen Unternehmen ihre eigenen Manager in Regress nehmen, in den letzten Jahren stark an. Der Vorwurf: Sorgfaltspflichtverletzungen oder mangelnde Risikoanalyse.

„Manager müssen im Zweifelsfall nachweisen, dass sie geeignete Vorsorgemaßnahmen getroffen haben und sie keine Schuld trifft“, sagt Jesko Trahms, Fachanwalt für Strafrecht und Partner bei BDO Legal Rechtsanwaltsgesellschaft mbH. „Ohne entsprechende Beweise ist das jedoch oft schwierig bis unmöglich – gerade bei Cybercrime oder Betrug. Auch beim Thema Compliance haben viele Unternehmen noch Nachholbedarf.“

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 Schutz 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 80 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. 2020 versicherte Euler Hermes weltweit Geschäftstransaktionen im Wert von EUR 824 Milliarden.

Weitere Informationen auf www.eulerhermes.de

Social Media

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.