Medieninformation

CORONAPANDEMIE: GEFAHR DURCH CYBERANGRIFFE STEIGT – 10 TIPPS, WIE SICH UNTERNEHMEN SCHÜTZEN KÖNNEN

- Verunsicherung und Covid-19 Informationsbedürfnis verleitet Mitarbeitende zu fatalen Klicks und öffnet Betrügern so Zugang zum Unternehmensnetzwerk
- Physische Distanz erhöht Erfolgschancen von Fake President Betrug
- Betrugsversuche flankiert von Whatsapp-Sprachnachrichten nehmen zu
- Zusätzliche Sicherheitsstufen: Bei höheren Finanztransaktionen ohne die Möglichkeit physischer Unterschriften ist teilweise ein 6-Augen-Prinzip sinnvoll sowie Rückruf-Verfahren zur Freigabe

Wallisellen, 14. Mai 2020 – Cyberkriminelle, falsche Chefs und Hacker haben aktuell die fast „perfekten" Arbeitsbedingungen. Fast überall arbeiten die Mitarbeitenden momentan aus dem Homeoffice, physisch getrennt von ihren Chefs und Teams. Das „Social Distancing" schafft perfekte Arbeitsbedingungen für „Social Engineers": Der Chefbetrug, auch unter Fake President oder CEO Fraud bekannt, arbeitet mit sogenanntem „Social Engineering", bei dem mit Hilfe von Wertschätzung und enormem Druck Mitarbeitende dazu gebracht werden, angeblich hochgeheime Finanztransaktionen zu tätigen.

„In Zeiten von Homeoffice ist es praktisch ausgeschlossen, dem Chef zufällig auf dem Flur zu begegnen und ihn auf die Transaktion anzusprechen", sagt Rüdiger Kirsch, Betrugsexperte bei Euler Hermes. „Das bedeutet, dass die Gefahr und die Erfolgsaussichten für den Chefbetrug in der aktuellen Situation enorm gestiegen sind. Zudem nutzen viele aktuell auch verstärkt informelle Kommunikationswege wie Whatsapp. Wir verzeichnen bereits die ersten Betrugsversuche, bei denen die betrügerischen E-Mails von Sprachnachrichten flankiert werden – um so das Vertrauen in die Echtheit des Chefs zu verstärken. Die Stimme war dabei zwar teilweise etwas verzerrt, aber ansonsten nah am echten Chef."

Verunsicherung durch Covid-19: Ein fataler Klick öffnet den Betrügern Tür und Tor
Neben der physischen Distanz spielt den Betrügern auch die Verunsicherung, Angst und das damit verbundene Informationsbedürfnis vieler Mitarbeiter in die Karten. Sie gelangen über Malware aktuell wesentlich leichter an ihr Ziel: ins Unternehmensnetzwerk. Statt sich aufwändig einzuhacken, öffnet ihnen Corona aktuell die Türen. Eine Website verspricht beispielsweise, Infektionen mit dem Coronavirus in Echtzeit auf einer Landkarte anzuzeigen, auch in der Schweiz. Wer darauf klickt, öffnet jedoch nicht nur die Karte, sondern lädt gleichzeitig im Hintergrund ein Malware-Programm herunter. Zudem kursieren vermehrt Phishing-Mails, die vorgeben, dass sie Video-Anweisungen zum Schutz vor Viren und aktuelle Entwicklungen hinsichtlich der Corona Bedrohung beinhalten. Auch die Weltgesundheitsorganisation WHO wird in Form gefälschter Informationsangebote und Verlautbarungen für kriminelle Machenschaften im Zuge der Corona-Epidemie missbraucht.

Einmal im Intranet, beobachten die Betrüger die Kommunikation, um verantwortliche Personen zu identifizieren, zum Beispiel in Finanzabteilungen. Zudem analysieren sie die Ansprache (Du/Sie), den Umgangston (formell/informell) und sonstige Gepflogenheiten, bevor sie dann ihre soziale Ingenieurskunst anwenden und zuschlagen.

Einfache Mittel oft am wirksamsten: Offene Kultur, Kommunikation und Sensibilisierung
„Die beste Schadensvermeidung ist eine offene Unternehmenskultur", sagt Kirsch. „Traut sich der Mitarbeitende, den Chef einfach anzusprechen, ist der Betrugsversuch bereits vereitelt. Je steiler die Hierarchien, desto grösser die Erfolgschancen der Betrüger. Besonders hierarchisch organisierte oder auch inhabergeführte Unternehmen sind überproportional häufig unter den Opfern des Chefbetrugs."

Neben der Unternehmenskultur ist jedoch vor allem die Sensibilisierung der Mitarbeitenden in der aktuellen Situation wichtiger denn je.

„Gerade jetzt sind solche Schulungen notwendig, auch wenn sie virtuell in manchen Unternehmen schwieriger oder aufwändiger zu organisieren sind als Anwesenheitsschulungen im Unternehmen selbst", sagt Kirsch. „Die Mitarbeitenden müssen sich der neuen Gefahren im Homeoffice bewusst sein, die häufig mit unaufgefordert erhaltenen Nachrichten zusammenhängen können, insbesondere der Zunahme von Phishing-Attacken im Zusammenhang mit Covid-19. Sonst öffnen sie den Betrügern mit einem Klick Tür und Tor."

Kommt es doch zu einem fatalen Klick, ist Zeit zumeist Geld. Auch hier spielt wieder die Unternehmenskultur eine Rolle. Trauen sich Mitarbeitende, dies zu melden, sind die Aussichten, dass schwerwiegende Folgen eintreten, wesentlich geringer.

6 Augen sehen mehr als 4: bei höheren Transaktionen kann mehrstufiges Prinzip sinnvoll sein
Wichtig ist, dass Unternehmen gerade in der Homeoffice-Situation alle Vorgaben, Anweisungen und Richtlinien uneingeschränkt aufrechterhalten, auch wenn dies teilweise umständlicher sein mag. Das 4-Augen-Prinzip gilt auch im Homeoffice.

"Bei höheren Finanztransaktionen macht es aktuell unter Umständen sogar Sinn ein 6-Augen-Prinzip einzuführen, da physische Unterschriften meist nicht mehr möglich sind", sagt Kirsch. "Zudem sollten Rückruf-Verfahren mit dem Vorgesetzten vor Freigabe von höheren Transaktionen eingeführt werden, damit eine weitere Sicherheitsstufe eingebaut wird. Letztlich spielt aber auch weiterhin die Wachsamkeit und das gute alte Bauchgefühl eine grosse Rolle."

Die «10 Tipps, wie sich Unternehmen in Zeiten von Corona vor Fake President schützen können:» finden Sie beigefügt oder hier zum Download.

Medienkontakt:
Euler Hermes Schweiz
Sylvie Ruppli
Communications Euler Hermes Schweiz
Tel. +41 44 283 65 14, sylvie.ruppli@eulerhermes.com

Euler Hermes ist weltweiter Marktführer im Kreditversicherungsbereich und anerkannter Spezialist in den Bereichen Kautionen, Garantien sowie Vertrauensschadenversicherung inkl. Cybercrime. Das Unternehmen verfügt über mehr als 100 Jahre Erfahrung und bietet seinen Business-to-Business(B2B)-Kunden Finanzdienstleistungen an, um sie im Liquiditäts- und Forderungsmanagement zu unterstützen. Über das unternehmenseigene Monitoringsystem wird täglich die Insolvenzentwicklung kleiner, mittlerer und multinationaler Unternehmen verfolgt und analysiert, die in Märkten tätig sind, auf die 92% des globalen BIP entfallen. Das Unternehmen mit Hauptsitz in Paris ist in 50 Ländern vertreten und beschäftigt mehr als 5‘800 Mitarbeitende. Euler Hermes ist eine Tochtergesellschaft der Allianz und wird von Standard & Poor’s mit einem Rating von AA bewertet. 2019 wies Euler Hermes einen konsolidierten Umsatz von EUR 2,9 Milliarden Euro aus und versicherte weltweit Geschäftstransaktionen im Wert von EUR 950 Milliarden.

Euler Hermes Schweiz beschäftigt rund 50 Mitarbeitende an ihrem Hauptsitz in Wallisellen und den weiteren Standorten in Lausanne und Lugano.

Weitere Informationen unter: www.eulerhermes.ch, LinkedIn oder Twitter @eulerhermes

Die Einschätzungen stehen wie immer unter den nachfolgend angegebenen Vorbehalten.
Vorbehalt bei Zukunftsaussagen: So weit wir hierin Prognosen oder Erwartungen äussern oder unsere Aussagen die Zukunft betreffen, können diese Aussagen mit bekannten und unbekannten Risiken und Ungewissheiten verbunden sein. Die tatsächlichen Ergebnisse und Entwicklungen können daher wesentlich von den geäusserten Erwartungen und Annahmen abweichen. Neben weiteren hier nicht aufgeführten Gründen ergeben sich eventuell Abweichungen aus Veränderungen der allgemeinen wirtschaftlichen Lage und der Wettbewerbssituation, vor allem in Allianz Kerngeschäftsfeldern und -märkten, aus Akquisitionen sowie der anschliessenden Integration von Unternehmen und aus Restrukturierungsmassnahmen. Abweichungen resultieren ferner aus dem Ausmass oder der Häufigkeit von Versicherungsfällen, Stornoraten, Sterblichkeits- und Krankheitsraten beziehungsweise -tendenzen, und insbesondere im Bankbereich aus dem Ausfall von Kreditnehmern. Auch die Entwicklungen der Finanzmärkte und der Wechselkurse, sowie nationale und internationale Gesetzesänderungen, insbesondere hinsichtlich steuerlicher Regelungen, können einen Einfluss ausüben. Terroranschläge und deren Folgen können die Wahrscheinlichkeit und das Ausmass von Abweichungen erhöhen. Die Gesellschaft übernimmt keine Verpflichtung, die hierin enthaltenen Aussagen zu aktualisieren.