CYBERKRIMINALITÄT: RISIKEN IM INTERNATIONALEN ZAHLUNGSVERKEHR

I. GESCHÄFTSAKTIVITÄT IN DER DIGITALEN WELT: VORSICHT GEBOTEN!

Heute verlagern sich immer mehr Geschäftsaktivitäten und berufliche Tätigkeiten in die digitale Welt. Die Coronavirus-Pandemie hat wesentlich zu diesem Trend beigetragen, da sie uns gezwungen hat, uns an neue Realitäten anzupassen. Diese Situation sowie die Effizienz und Bequemlichkeit des Remote Work haben eine neue Arbeitsrealität geschaffen, die wiederum neue Risiken mit sich bringt, derer sich viele von uns vorher nicht bewusst waren. Die Rede ist von der Cyberkriminalität, der insbesondere immer mehr Unternehmen zum Opfer fallen. Besonders in letzter Zeit ist eine Zunahme dieser Art von Kriminalität zu beobachten.

II. MODUS OPERANDI DER CYBERKRIMINELLEN

Eine häufig von Tätern angewandte Methode ist der Versuch, sich durch gefälschte E-Mail-Adressen als reguläre Geschäftspartner eines Unternehmens auszugeben, um Kontonummern zu ändern, auf die Zahlungen im Zusammenhang mit Transaktionen überwiesen werden. In den meisten Fällen wird bei der Fälschung nur ein Buchstabe der ursprünglichen (korrekten) E-Mail-Adresse geändert, so dass die Änderung nicht leicht zu erkennen ist. Die Relevanz dieses Themas muss hervorgehoben werden: Fällt ein Unternehmen zum Opfer einer solchen Straftat, zieht sich das Strafverfahren oft über Jahre hin. Dies liegt nicht nur an der Schwierigkeit, die Täter zu ermitteln, sondern in vielen Fällen auch an der Notwendigkeit, Verfahren in Zusammenarbeit mit Behörden in anderen Ländern einzuleiten. Diese Notwendigkeit ergibt sich aus der Tatsache, dass Täter dieser Art von Straftaten meistens kriminelle Gruppen sind, die in und aus mehreren Ländern operieren. Wird ein Cybercrime innerhalb der EU begangen, lässt sich dies als weniger problematisch betrachten. Handelt es sich jedoch um einen Vorfall, an dem Drittländer beteiligt sind, können ersthafte Probleme entstehen, weil eine Zusammenarbeit zwischen den zuständigen Staatsanwaltschaften praktisch unmöglich erscheint.

III. BESSER VORBEUGEN ALS NACHTRÄGLICH SCHADEN BEGRENZEN

Durch Vorsichtsmaßnahmen kann das Risiko minimiert werden. Schon allein dadurch, dass in Verträge mit den Vertragspartnern genaue Bankverbindungsdaten aufgenommen werden. Änderungen dieser Angaben könnten folglich nur auf der Grundlage eines Nachtrags vorgenommen werden. In jeder Situation, die zu einer Änderung der Kontonummer führen kann, sollte genau nachgeprüft werden, ob beispielsweise das neue Bankkonto des Geschäftspartners in dem Land geführt wird, in dem er tatsächlich tätig ist.

Bei einem Wechsel des Bankkontos sind zusätzliche Kontrollen zu empfehlen, insbesondere durch die Geschäftsleitung, um die Echtheit solcher Änderungen festzustellen. Auf jeden Fall ist immer darauf aufmerksam zu machen, wie wichtig es ist, über unternehmensinterne Verfahren, einschließlich Arbeitsordnung und sonstiger innerbetrieblicher Regelungen für den Fall eines Betrugsversuchs zu verfügen, sowie Schulungen für Mitarbeiter durchzuführen, um

sie auf mögliche Cyber-Bedrohungen vorzubereiten und zu sensibilisieren.

IV. SCHNELLE REAKTION AUF CYBER-VORFALL

Ist man Opfer einer solchen Straftat geworden, ist es am wichtigsten, umgehend zu handeln. Die Erfahrung zeigt, dass Mitarbeiter, die in einen solchen Cyberbetrug verwickelt sind, oft eine Art Scham über ihr eigenes Verhalten empfinden und versuchen, mit den Tätern direkt in Kontakt zu treten. Da hier aber jede Stunde zählt, sollten die Mitarbeiter sensibilisiert werden, nicht auf eigene Faust zu handeln, denn in einem solchen Fall ist es nicht nur wichtig, schnell, sondern auch angemessen vorzugehen. Zuallererst ist die eigene Bank, bei der das Geschäftskonto geführt wird, so schnell wie möglich zu benachrichtigen, um (wenn noch möglich) Überweisungen auf das gefälschte Bankkonto zu stoppen. Können die überwiesenen Geldmittel leider nicht mehr von der Bank zurückgeholt werden, müssen umgehend rechtliche Schritte eingeleitet werden.

Haben Sie Fragen zum Thema Cyber-Kriminalität oder benötigen Sie juristische Unterstützung bei einem Cyber-Vorfall, lassen Sie sich bitte von unseren erfahrenen Experten beraten.

KONTAKT

Bulgarien
Cornelia Draganova
Cornelia.Draganova@schindhelm.com

China
Marcel Brinkmann
Marcel.Brinkmann@schindhelm.com

Deutschland
Rüdiger Erfurt
Ruediger.Erfurt@schindhelm.com

Frankreich
Maurice Hartmann
Maurice.Hartmann@schindhelm.com

Italien
Tommaso Olivieri
Tommaso.Olivieri@schindhelm.com

Österreich
Philipp Leitner
P.Leitner@scwp.com

Polen
Konrad Schampera
Konrad.Schampera@sdzlegal.pl

Rumänien
Stefan Pisargeac
Stefan.Pisargeac@schindhelm.com

Spanien
Axel Roth
A.Roth@schindhelm.com

Tschechien/Slowakei
Monika Wetzlerova
Wetzlerova@scwp.cz

Türkei
Gürkan Erdebil
Gurkan.Erdebil@schindhelm.com

Ungarn
Beatrix Fakó
B.Fako@scwp.hu

Herausgeber, Medieninhaber, Redaktion: Zimányi & Fakó Rechtsanwälte | Lövőház u. 30 | 1024 Budapest | Registernummer: 2019 | Register: Budapester Anwaltskammer (H-1055 Budapest, Szalay u. 7.) | Tel: +36 1 270-9242, Fax: +36 1 270-9241 | budapest@scwp.com | Zimányi & Fakó Rechtsanwälte ist Mitglied der Saxinger Schindhelm Services SE, Allianz europäischer Wirtschaftskanzleien | Alle Angaben erfolgen trotz sorgfältiger Bearbeitung ohne Gewähr und können im Einzelfall die individuelle Beratung nicht ersetzen. Die Haftung der Autoren oder der Herausgeberin ist ausgeschlossen. | 2015 © Zimányi és Fakó Ügyvédi Iroda