Optionen für den Ernstfall

Was tun bei Cyberbetrug?

Angriffe von Cyberkriminellen sind alltägliche Realität. Häufig sind Unternehmen dabei direkt das Ziel. Firmen und ihre Reputation können aber auch bei Attacken auf Einzelpersonen indirekt betroffen sein. Wir zeigen mögliche Handlungsoptionen auf.

→ VON MARC FELDMANN UND ALEXANDER HOFMANN

DIE AUTOREN

Marc Feldmann
ist Legal Engineer bei Laux Lawyers.

Alexander Hofmann
ist Rechtsanwalt und Senior Advisor bei Laux Lawyers. Zudem ist er Mitglied der Rechtskommission von swissICT. In der Kolumne «Recht & IT» berichten Mitglieder der Kommission über aktuelle juristische Themen im digitalen Bereich.
→ **www.swissict.ch**

Gängige Betrugsversuche gegen Einzelpersonen sind etwa das Cybersquatting (Imitation bestehender Originaldomains) oder auch sogenannte Scams, wo in Zusammenhang mit vorgetäuschten Erbschaften, Lotteriegewinnen oder auch Jobangeboten die Identität von Anwaltskanzleien, Banken oder der vermeintlichen Anbieterin vorgespielt wird. Von solchen «Identitätsklaus» betroffene Firmen sollten nicht untätig bleiben, sondern aktiv mögliche Gegenmassnahmen prüfen und allenfalls umsetzen.

MISSBRAUCH MELDEN

Betroffene können den Missbrauch bei der zuständigen Domain-Registrierungsstelle melden. Deren Identität lässt sich durch eine «Whois-Abfrage» in Erfahrung bringen. Enthalten gefälschte Domains markenrechtlich geschützte Elemente, besteht zusätzlich unter anderem die Möglichkeit, über das «Domain Name Dispute Resolution»-Verfahren der Weltorganisation für geistiges Eigentum die Löschung der gefälschten Domain zu erlangen. Ob sich dies lohnt, ist im Einzelfall und mit Blick auf die Kosten abzuwägen.

FAKE-KONTEN UND RUFNUMMERN SPERREN LASSEN

In vielen Fällen werden Scam-E-Mails wahllos an unzählige Adressen versandt. Dazu werden entweder gekaperte (private) Accounts oder kostenlose E-Mail-Adressen verwendet. Zuweilen werden potenzielle Opfer auch über Posts oder Nachrichten auf Social-Media-Plattformen wie Facebook, Instagram und LinkedIn oder Messenger-Dienste wie WhatsApp oder Telegram kontaktiert. Die meisten Anbieterinnen bieten hierbei niederschwellige und kostenfreie Möglichkeiten, um gefälschte oder imitierende Konten zu melden. Informationen zum genauen Vorgehen finden sich jeweils in den FAQs oder auf Hilfe-Seiten der Dienste. Der geringe Aufwand spricht für solche Meldungen; es muss jedoch damit gerechnet werden, dass die Kriminellen bald auf eine neue Identität ausweichen.

Besonders dreiste Scammer nutzen gar gültige lokale Telefonnummern für ihre Angriffe. Da sie sich meist im Ausland aufhalten, werden die Nummern über VoIP-Angebote wie Skype genutzt. Leider lässt sich aus den öffentlich verfügbaren Registern nur selten eruieren, welcher VoIP-Anbieterin der Missbrauch zu melden wäre. Es bleibt somit einzig der Weg über eine Strafanzeige oder der Versuch, die gängigsten Anbieterinnen «auf gut Glück» anzuschreiben.

STRAFANZEIGE EINREICHEN

In jedem Fall besteht auch die Möglichkeit, eine Strafanzeige einzureichen. Allerdings lässt sich oft nicht feststellen, wer hinter den missbräuchlich verwendeten Domains oder Accounts steht, wodurch eine Anzeige (gegen Unbekannt) nur selten zu einer erfolgreichen Strafverfolgung führen wird. Sie kann aus zwei Gründen trotzdem sinnvoll sein: Einerseits kann damit gezeigt werden, dass sich Betroffene im Kampf gegen Cyberbetrug aktiv bemühen. Andererseits werden auch Statistiken über angezeigte Straftaten geführt, was wiederum über den politischen Weg zu einem Ausbau des rechtlichen Instrumentariums führen kann.

TRANSPARENZ SCHAFFEN

Die Erfahrung zeigt schliesslich, dass Betroffene oft Verdacht schöpfen und versuchen, sich an die vermeintlichen Absenderinnen direkt zu wenden. Deshalb empfehlen wir als zusätzliche Massnahme, auf der eigenen Website über bekannte Betrugsfälle zu informieren. Dabei sollte insbesondere erläutert werden, wie die Betrüger vorgehen und wie ein Betrug erkannt werden kann. Solche Einträge können dann von Betroffenen auch über Suchmaschinen gefunden werden und aufklären. Dies kann zudem (individuell betrachtet) den willkommenen Nebeneffekt haben, dass Kriminelle auf andere Unternehmen ausweichen. ←

> «Betroffene Firmen sollten nicht untätig bleiben, sondern aktiv mögliche Gegenmassnahmen prüfen und allenfalls umsetzen»
>
> Marc Feldmann und Alexander Hofmann