HINTERGRUNDBERICHT

Social Engineering auf Firmenebene

Seit Jahren prasselt eine Menge von immer besser ausgearbeiteten Betrugsmaschen auf alle privaten Internetnutzer ein. Betrugsmaschen wie die angeblichen Anrufe von Microsoft Mitarbeitern, gefälschte DHL-Mails und ähnliche nutzen die Methoden des Social Engineering um Gelder unrechtmäßig zu erbeuten. Vor etwa einem Jahr konnte die Corporate Trust in ihren Fällen erste Betrugsmaschen erkennen, die sich auf Unternehmen spezialisiert haben. Seit einigen Monaten beobachten wir eine exponentielle Zunahme solcher Fälle:

„Fake President"

Bei dieser Betrugsmasche geben sich die Täter als ein Organ des versicherten Unternehmens - meist ein Vorstandsmitglied - aus und bitten per E-Mail oder Fax einen Mitarbeiter, der im Unternehmen Bankgeschäfte durchführen darf, eine dringende Überweisung auszuführen. Dem Mitarbeiter wird dabei vorgespiegelt, dass es sich um eine höchst geheime und vertrauliche Angelegenheit handelt, von der strategische Weichenstellungen im Unternehmen abhängen. Die Betroffenen, die sich einerseits aufgrund des besonderen Vertrauens durch den Vorstand geschmeichelt fühlen, anderseits aufgrund der angeblichen Wichtigkeit der Transaktion erheblich unter Druck stehen, führen diese Überweisungen meist zügig aus. Fast immer erfolgen die Geldtransfers auf ausländische Konten, vor allem in Asien und Osteuropa. Fliegt der Betrug dann auf, sind die Konten dort meist leergeräumt oder eine Rückholung wird aufgrund des ausländischen Rechtssystems erheblich erschwert. Die E-Mails kommen oft von externen Adressen (z.B. Google Mail) mit den korrekten Namen des vermeintlichen Vorstandsmitglieds – in der E-Mail wird dann argumentiert, die Angelegenheit sei so vertraulich bzw. dringend, dass hierfür bitte dieser Privataccount zu nutzen sei. Oft geht die Mail in CC an die echte Adresse des Vorstands – allerdings mit einem kleinen Schreibfehler, sodass die Mail nicht wirklich ankommt.

Häufig werden gezielt Mitarbeiter bzw. Geschäftsführer in ausländischen Niederlassungen des Unternehmens angesprochen. Das erschwert den Mitarbeitern die persönliche Kontaktaufnahme mit den verantwortlichen Organen im Unternehmen, von denen die vermeintlichen Anweisungen kommen.

„Payment Diversion"

In diesen Fällen geben sich die Betrüger als Geschäftspartner oder Lieferanten des Unternehmens aus und erreichen durch gefälschte Mitteilungen, dass die Bezahlung für Waren oder erbrachte Dienstleistungen auf abweichende Konten erfolgt. Die Umsetzung dieser Form des Betruges wird ermöglicht durch eine gefälschte Mitteilung an das Unternehmen, dass sich die bisher vereinbarten Bankverbindungen geändert haben und der Zahlungsverkehr nun über die neue Bankverbindung abgewickelt werden soll.

„Fake Identity Fraud"

Auch bei diesem Betrugsszenario geben sich die Täter als ein bereits existierender Kunde oder als ein Neukunde des Unternehmens aus und ordern schriftlich Waren. Mit plausiblen Erklärungen wird dann die Lieferung an eine abweichende Lieferadresse verlangt. Da die Identität einer tatsächlich existierenden Firma genutzt wird, schöpfen die Betrugsopfer zunächst keinen Verdacht. Oft fliegt der Betrug erst dann auf, wenn Zahlungsverzug eintritt und die tatsächlich existierende Firma gemahnt wird. Wird dann die Lieferadresse durch die Polizei überprüft, werden die Geschäftsräume verlassen vorgefunden und die Ware ist selbstverständlich längst weiter verschoben worden.

Die einzig wirklich effektive Maßnahme gegen diese Betrugsmasche sind wachsame Mitarbeiter. Wir empfehlen jeder Firma diese Betrugsszenarien allen Mitarbeitern die Bankgeschäfte oder Adressänderungen auslösen dürfen, bekannt zu machen. Die Corporate Trust hat diesbezüglich gute Erfahrungen mit der Durchführung von „Fraud Workshops" gemacht, die ganze Abteilungen auf diese und zukünftige Betrugsszenarien vorbereiten.

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Zieher Business Center | Rosenstraße 2 | 10178 Berlin
Telefon +49 (0)30 200 77 200 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de