CHUBB®

Risk Newsletter

Wenn Mitarbeiter zur Cyber-Zielscheibe werden

Wie verwundbar ist eigentlich eine Gesellschaft, die sich zunehmend digitalisiert? „Sehr stark“ lautet hier inzwischen die Antwort, denn im Cyberbereich entwickeln sich fast täglich neue Risiken, die allesamt mit einem erheblichen Schadenpotenzial einhergehen können. Gemeint sind hiermit technologische Lücken im Unternehmen, verstärkt aber auch der Faktor Mensch, der zur Gefahr werden kann. Denn die Belegschaft eines Unternehmens stellt aus der Sicht von Kriminellen immer das schwächste Glied in der IT-Sicherheitskette dar und so zielen sie immer häufiger auf die „Schwachstelle“ Mensch, um die sonst gängigen Sicherheitsvorkehrungen eines Unternehmens zu umgehen und an sensible Informationen, Daten oder nicht zuletzt natürlich auch an Geld zu gelangen.

Ausgeklügelt und hochprofessionell

Digitaler Betrug befindet sich auf dem Vormarsch und derzeit populärster Vorgehensweise hierbei ist der sogenannte Fake President Fraud, alternativ auch als CEO Fraud bekannt: Die Täter geben sich als Mitglied der Chefetage aus - beispielsweise als Geschäftsführer, Chief Financial Officer oder aber auch als Anwalt der Firma -, um Mitarbeiterinnen und Mitarbeiter meist aus der Finanzabteilung des Unternehmens entweder per E-Mail oder Telefon zur Überweisung größerer Geldbeträge ins Ausland zu verleiten. Äußerst koordiniert und professionell gehen die Cyberkriminellen dabei vor, greifen bei ihrer Betrugsmethode sogar auf Insiderinformationen über das Unternehmen zurück. Oftmals hacken sie zunächst mehrere E-Mail-Accounts der Firma und spähen diese sorgfältig über Wochen oder sogar Monate hinweg aus. Auch etwaige Informationen zur Firmenstruktur, die auf der Homepage des Unternehmens frei zugänglich abrufbar sind, oder nähere Berufsangaben von Mitarbeiterinnen und Mitarbeitern aus öffentlichen Berufsnetzwerken können den Cyberkriminellen für ihre Zwecke dienen. Mit dem umfassenden Wissen um interne Unternehmensabläufe, -hierachien und -strukturen, eine geschickte Kommunikation sowie vor allem natürlich auch durch die richtige E-Mail-Adresse des Absenders treten sie authentisch auf und zerstreuen damit eventuelle Zweifel der betroffenen Mitarbeiterinnen und Mitarbeiter.

Falscher Chef, realer Schaden

Längst ist Fake President Fraud kein Problem mehr, das vor allem beispielsweise den US-amerikanischen Markt betrifft, wo diese Art des Betrugs bereits seit einigen Jahren verbreitet ist. Inzwischen geraten Unternehmen weltweit ins Visier - immer häufiger gerade auch deutsche. Sind die Kriminellen mit dem digitalen Betrug erfolgreich, können die finanziellen Folgen für das betroffene Unternehmen enorm sein, denn Schäden in Millionenhöhe sind beim Fake President Fraud keine Seltenheit. Über 150 Millionen Euro wurden allein in Deutschland innerhalb der letzten zwei Jahre erbeutet, wie aus den bundesweit ▶

gemeldeten Betrugsfällen, die über eine Vertrauensschadenversicherung abgedeckt wurden, hervorgeht. Zudem gehen Experten bei diesem Phänomen von einer erheblichen Dunkelziffer aus. Umso entscheidender ist es angesichts der zunehmenden Bedrohung daher, dass es erst gar nicht zu solch einem Vorfall im eigenen Unternehmen kommt.

Ohne Sensibilisierung keine Sicherheit

Ein umfassendes Risk Management gestaltet sich beim Thema Cybersicherheit als Schlüsselfaktor – sowohl im Hinblick auf umfangreiche technische als auch organisatorische Schutzmaßnahmen. Von zentraler Bedeutung ist hierbei vor allem die Mitarbeiterinnen und Mitarbeiter für digitale Gefahren zu sensibilisieren und sie entsprechend dafür zu schulen. Denn anders als bei anderen Unternehmensrisiken sind die Bedrohungen im Cyberbereich oftmals nicht sofort zu erkennen, da sie meist abstrakt und nicht tatsächlich greifbar sind. Nicht selten unterschätzen viele daher die Bedrohungslage der heutigen digitalen Welt oder aber sind sich häufig gar nicht der Bedeutung, genauer gesagt dem Wert von sensiblen Daten und Information bewusst.

Regelmäßig auf aktuelle digitale Gefahren hinzuweisen, damit potentielle Angriffsversuche von Mitarbeiterinnen und Mitarbeitern erkannt und daraufhin natürlich auch richtig gehandhabt werden können, trägt schon maßgeblich dazu bei, das Risiko einer Infektion des Unternehmensnetzwerks oder eines Betruges zu verringern. Tatsache ist nämlich, dass jede noch so gute IT-Sicherheitslösung durch Unachtsamkeit oder Fehlverhalten, durch mangelndes Bewusstsein und fehlende Kenntnis auf Seiten der Belegschaft schlichtweg ihre Wirkung verliert. Genau diese Tatsache macht digitale Risiken für Unternehmen so schwierig zu handhaben – und damit so gefährlich.

Jana Dünkeloh
Manager Commercial Risks Deutschland & Österreich, Financial Lines
jana.duenkeloh@chubb.com

Chubb. Insured.℠