Betrugsfall bei LEONI: Hintergründe und Empfehlungen

17.8.2016 – Eine nun seit über einem Jahr zu beobachtende Betrugsmasche, die Aufgrund der charakteristischen Vorgehensweise der Betrüger meist "Fake President Angriff" genannt wird, fand wohl in der Nürnberger LEONI AG jüngst ein weiteres, bekanntes Opfer. Warum fällt es nach wie vor vielen Unternehmen schwer, sich gegen derartige "Social Engineering" Angriffe wirksam zu schützen?

Aktuell zeichnet sich im europäischen Raum ein deutlicher Anstieg spezifischer Betrugsfälle ab. Diese sind aufgrund ihrer professionellen und zielgerichteten Durchführung der organisierten Kriminalität zuzuschreiben. Den Betrugsfällen gehen oft monatelange Recherchen voraus, woraufhin mit gezielten Social-Engineering-Angriffen die schwächsten Glieder der Kette in Unternehmen – die Mitarbeiter – getäuscht und dadurch Schäden verursacht werden, welche teilweise in die Millionen gehen. Bei der LEONI AG waren es wohl nun 40 Mio. EUR, bei der FACC AG waren es Ende 2015 50 Mio EUR. Das Geld wird schnell auf ausländische Konten transferiert, die Aktien verlieren nach der Bekanntgabe meist sofort an Wert, die LEONI Aktie 9% binnen einer Stunde.

Laut einem Bericht des Focus heißt es aus dem Firmenumfeld, jemand habe sich mittels "betrügerischer Handlungen, Verwendung gefälschter Dokumente und Identitäten sowie Nutzung elektronischer Kommunikationswege" offenbar erfolgreich als Leoni-Mitarbeiter mit "besonderen Befugnissen" ausgegeben und auf diese Weise "bestimmte Geschäftsvorgänge vorbereiten" lassen, die am Ende dazu führten dass Gelder des Unternehmens im Umfang von 40 Millionen Euro auf Zielkonten im Ausland transferiert wurden.

Derartige Betrugsmaschen treffen eine Achillesferse der Wirtschaft: Geschäftsabläufe müssen schnell und effizient sein, Email ist das primäre Kommunikationsmedium (obwohl es keine Authentizität garantieren kann) und der Hierarchie wird oft blind vertraut. Die komplexen Strukturen großer Unternehmen mit ihren Hürden in der Kommunikation zwischen verschiedenen Unternehmenseinheiten und Hierarchiestufen bilden dabei eine gute Grundlage für solche Betrugsfälle. Zusätzlich sorgt Routine im Betriebsablauf in vielen Fällen für eine gewisse Art von Betriebsblindheit, wodurch im Zuge der Standardprozesse häufig kein Misstrauen bei den ausgewählten Mitarbeitern erweckt wird.

Kern dieser Betrugsmaschen ist klassisches Social Engineering, gepaart mit einer vorausgehenden, intensiven Ausforschung der Unternehmenshierarchie sowie der aktueller Geschäftsprozesse des Opfers. Dabei gibt es mehrere Szenarien - den Berichten zufolge hat es die LEONI AG mit dem häufigsten der drei ähnlichen Betrugsszenarien erwischt: dem „Fake President“.

Szenario 1: „Fake President“ – Vortäuschung einer falschen Identität

WAS?

- Bei diesem Betrugsszenario erhalten bevollmächtigte Mitarbeiter – vornehmlich international agierender Unternehmen – unter dem Vorwand eines bevorstehenden und geheimen M&A-Vorhabens die Aufforderung, eine vermeintlich dringende und geheime Finanztransaktion auf ein ausländisches Konto durchzuführen.

WER?

- **Täter** geben sich als hochrangige Manager (meist auf Vorstandsebene des Unternehmens) aus.

- **Opfer** sind in der Regel Mitarbeiter, welche für Bankgeschäfte beziehungsweise Finanztransaktionen bevollmächtigt sind.

WIE?

- Die Kontaktaufnahme erfolgt zunächst schriftlich, zum Beispiel per E-Mail oder Fax, durch gefälschte Absenderadressen, welche sich auf den ersten Blick kaum vom echten Format unterscheiden lassen.
- Oft wird ein vermeintlicher Anwalt, Steuerberater, Wirtschaftsprüfer oder Notar in cc gesetzt, um dem Schreiben mehr Authentizität zu verleihen.
- Anschließend erhalten die Opfer auch Anrufe der vermeintlichen Anwälte, um die Glaubwürdigkeit zu bekräftigen.

PROBLEM

- Durch die Vorspiegelung einer vermeintlich streng geheimen, unternehmenskritischen und strategisch wichtigen Angelegenheit fühlen sich die Opfer geschmeichelt und verpflichtet.
- Aufgrund der Dringlichkeit der Angelegenheit stehen die Opfer unter Druck und führen die Überweisungen meist zügig und ohne Rücksprache aus.
- Da sich die Zielkonten vornehmlich in Osteuropa beziehungsweise Asien befinden, sind diese nach Betrugserkennung zumeist leer geräumt, während das jeweilige Rechtssystem die Rückholung der Summen erheblich erschwert.

Szenario 2: „Payment Diversion“ – Umleitung von Zahlungsverkehr

WAS?

- Bei diesem Betrugsszenario werden ausgewählten Mitarbeitern durch angebliche Geschäftspartner oder Zulieferer geänderte Bankdaten übermittelt, mit der Aufforderung, diese im zukünftigen Zahlungsverkehr zu berücksichtigen.

WER?

- **Täter** geben sich als Geschäftspartner oder Lieferanten aus.
- **Opfer** sind in der Regel Mitarbeiter, welche zur Verwaltung beziehungsweise Veränderung von Bankdaten berechtigt sind.

WIE?

- Die Kontaktaufnahme seitens der Täter erfolgt in der Regel schriftlich via E-Mail, Fax oder Brief und in manchen Fällen auch telefonisch. Dabei wird auf professionelle Art und Weise die Identität beziehungsweise Unterschrift des jeweiligen Geschäftspartners oder Lieferanten gefälscht.

PROBLEM

- Durch die Änderung der Bankdaten ist die Rechnungslegung für zukünftige Waren oder Dienstleistungen manipuliert.
- Der Betrug fällt in der Regel erst dann auf, wenn Zahlungserinnerungen oder gar Mahnungen seitens des echten Geschäftspartners/Lieferanten beim betroffenen Unternehmen eintreffen.

Szenario 3: „Fake Identity Fraud“ – Umleitung von Warenverkehr

WAS?

- Bei diesem Betrugsszenario werden ausgewählte Mitarbeiter durch vermeintliche Bestandskunden mit einem Stammdatenänderungsantrag kontaktiert.

WER?

- **Täter** geben sich als Bestandskunde, seltener auch als Neukunde aus.
- **Opfer** sind in der Regel Mitarbeiter, welche zur Verwaltung beziehungsweise Veränderung von Stammdaten berechtigt sind.

WIE?

- Die Kontaktaufnahme seitens der Täter erfolgt in der Regel schriftlich via E-Mail, Fax oder Brief. In manchen Fällen geht dem ein Telefonat voraus. Dabei wird auf professionelle Art und Weise die Identität beziehungsweise Unterschrift des jeweiligen Geschäftspartners oder Kunden gefälscht.

PROBLEM

- Durch die plausibel wirkende Angabe abweichender Lieferadressen werden Waren an die Täter geliefert.
- Der Betrug fällt oft erst bei Zahlungsverzug beziehungsweise Mahnung der tatsächlichen Firma auf.

Empfehlungen der Corporate Trust (präventiv)

- **Schaffen Sie klare Prozesse und Zuständigkeiten:**
  - Etablieren Sie bei relevanten Finanztransaktionen ein Vier-Augen-Prinzip.
  - Regeln Sie, wie im Anlassfall bei ungewöhnlich hohen oder dringenden Zahlungen vorzugehen ist.
  - Sorgen Sie dafür, dass Ihre IT die Mitarbeiterberechtigungen auf das Nötigste reduziert.
  - Überprüfen Sie regelmäßig die Einhaltung der Arbeitsanweisungen.

- **Prüfen Sie die vermeintlichen Zahlungsaufforderungen auf ihre Glaubwürdigkeit:**
  - Verifizieren Sie die Identität des Absenders per Telefon oder E-Mail.
  - Verwenden Sie bei der Verifikation nicht die Kontaktdaten aus der E-Mail oder dem Telefonat. Ziehen Sie stattdessen interne Aufzeichnungen beziehungsweise die Firmenwebseite heran.

- **Schaffen Sie bei Ihren Mitarbeitern Bewusstsein für die Gefahren:**
  - Organisieren Sie Awareness-Trainings und sensibilisieren Sie Ihre Mitarbeiter bezüglich verdächtiger Anschreiben (Inhalt, Schreibstil, unüblicher Wortlaut).
  - Senden Sie ein Rundschreiben, in welchem Sie Ihre Mitarbeiter über die aktuellen Betrugsfälle aufklären.
  - Schließen Sie eine Fraud-Versicherung ab: Versicherungen bieten spezialisierte Pakete an, welche Ihnen im Betrugsfall den entstandenen Schaden zumindest teilweise rückerstatten.

Empfehlungen der Corporate Trust im Fall der Fälle

- **Kontaktieren Sie (beispielsweise über Ihren Anwalt) die Empfängerbank und lassen Sie die entsprechenden Beträge auf dem Zielkonto einfrieren.**
  - Wenn das Konto bereits leergeräumt ist, lassen Sie sich Informationen zur Weiterleitung geben.

- **Kontaktieren Sie die zuständige Geldwäschebehörde im Zielland der Transaktion und lassen Sie die entsprechenden Beträge auf dem Zielkonto einfrieren.**
  - Lassen Sie sich im Falle einer bereits erfolgten Weiterleitung des Geldes die Informationen zum Zielkonto beziehungsweise zur Empfängerbank geben, um den Geldfluss nachvollziehen zu können.

- **Erstatten Sie Anzeige bei der Kriminalpolizei, Staatsanwaltschaft beziehungsweise Ihrer zuständigen Geldwäschebehörde:**
  - Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) mit Sitz in Frankfurt am Main/Bonn

Maßnahmen mit hoher Managementaufmerksamkeit

Realistisch und ehrlich betrachtet sind die oben beschriebenen Maßnahmen das, was Unternehmen sinnvoll gegen die genannten Betrugsfälle tun können. Vor allem nach einem solchen Betrugsfall entsprechen diese Maßnahmen meist nicht dem, was das Management erwartet. Nachfolgend aufgeführte Empfehlungen helfen bei den Betrugsfällen meist wenig, bringen aber dem Unternehmen eine transparente und dadurch glaubhafte Sicht auf das aktuelle Sicherheitsniveau des Unternehmens und können in seltenen Fällen bei der Aufklärung helfen.

- IT-Security-Quickcheck
- Anti-Fraud-Workshop
- Prävention für Forensik
- Spionage-Penetrationstest

Über Corporate Trust, Business Risk & Crisis Management GmbH

Corporate Trust ist der strategische Partner namhafter Unternehmen im Risiko- und Krisenmanagement. Als Unternehmensberatung für Sicherheitsdienstleistungen unterstützt Corporate Trust Unternehmen, Organisationen und Privatpersonen im High-Level-Security-Bereich.

Sicherheitskonzepte sollten so effektiv und diskret sein, dass ihre Existenz am besten gar nicht wahrgenommen wird. Genau das ist die Mission. Corporate Trust will eine Umgebung schaffen, in der man sich absolut sicher und ungestört auf die eigenen Ziele und die Ziele des Unternehmens konzentrieren kann. Im Mittelpunkt steht dabei immer der Mensch.

Ansprechpartner:

Dipl.-Inf. Florian Oelmaier
Leiter Cyber-Sicherheit und Computerkriminalität
Tel. 089-599 88 75 80
oelmaier@corporate-trust.de
https://www.corporate-trust.de