CB-BEITRAG

Thomas Fritzsche

Eigenschaften von Fake President Fraud – Grundlagen zur Risikobeurteilung, Maßnahmenableitung und Reaktion im Ernstfall

Dieser Beitrag führt in die Charakteristika eines erfolgreichen Fake President-Angriffs ein. Die umfassende Betrachtungsweise schafft die Basis für einen ausgewogenen Dialog zur Beurteilung und Behandlung dieses wachsenden Risikos für Unternehmen aller Branchen und Größenordnungen.

I. Einleitung

Die Betrugsmasche „Fake President" wird zunehmend in deutschen und internationalen Unternehmen diskutiert. Schadenssummen von zuletzt großen zweistelligen Millionenbeträgen lenken den Blick von Vorständen und Geschäftsführern, aber auch Abteilungen wie Finanzen, Buchhaltung, Compliance, Recht und Informationssicherheit auf diese etablierte Form der Wirtschaftskriminalität. Auch wenn das Angriffsmuster selbst nicht neu ist, so ist dennoch Dynamik rund um dieses Risiko entstanden. Bei Versicherungsunternehmen rangiert der Fake President Fraud auf den obersten Rängen der aktuellen Betrugsszenarien. Einige Versicherungsunternehmen reagierten mit der Anpassung ihrer Bedingungswerke auf das erneute Aufflammen der alten Betrugsmasche. Grob fahrlässiges Verhalten von Mitarbeitern ist nun kein Ausschlusskriterium mehr für das Einspringen einer Vertrauensschadenversicherung. Auch die Deckelung beim Betrug durch Externe wurde teilweise gesenkt. Zu berücksichtigen ist zudem, dass ein Fake President-Vorfall möglicherweise auch in den Deckungsbereich einer D&O-Versicherung fallen kann, sofern die Frage nach einer möglichen Pflichtverletzung des Vorstands in Bezug auf sichere Zahlungsprozesse zu klären ist. Auf der anderen Seite hat bspw. das Sächsische Landesarbeitsgericht eine Arbeitnehmerin zum Schadensersatz verurteilt (Sächsisches LAG vom 13.06.2017, Az. 3 Sa 556/16). Das Urteil zeigt das Spannungsfeld in der Beurteilung von grob fahrlässigem Verhalten der in den Vorfall involvierten Mitarbeitern einerseits und der Ausgestaltung von Schutzmaßnahmen gegen Fake President-Betrug im Unternehmen anderseits.

Der Gestaltung sicherer Zahlungsprozesse fällt in Unternehmen daher eine entsprechende Bedeutung zu. Aktuelle Diskussionen sind nach wie vor zu stark auf die eher trivialen Angriffsszenarien fokussiert. Der besonderen Situation eines in den Vorfall involvierten Mitarbeiters[1] wird damit nicht ausreichend Rechnung getragen. Die Strategie der Betrugsmasche ist jedoch auf die Umgehung bzw. unautorisierte Nutzung von vorhandenen Prozessen durch geschickte Täuschung eines Mitarbeiters der Abteilung Finanzen oder der Buchhaltung ausgelegt. Dabei ist die Ausnutzung menschlicher Eigenschaften ein zentrales Element der technologisch und psychologisch versierten bis hochprofessionellen Angreifer. Das Management und die Mitarbeiter mit Kompetenz zur Zahlungsautorisierung und -anweisung sollten neben sicheren Prozessen im Zentrum jeder Risikobetrachtung stehen. Für eine fundierte und umfassende Diskussion und Maßnahmenableitung lohnt sich daher die Betrachtung der Eigenschaften eines idealtypischen Fake President-Vorfalls.

II. Begriffliche Einführung

Der sog. Fake President Fraud ist auch unter anderen Bezeichnungen wie CEO-Fraud, Enkeltrick 2.0 oder auch Chef-Masche bekannt. Der Beitrag verwendet im Folgenden die Kurzform „Fake President". Dabei versuchen externe Angreifer einen Mitarbeiter der Abteilung Finanzen oder der Buchhaltung zur Überweisung von großen Beträgen ins Ausland zu bewegen, wobei große Eile geboten ist. Dabei wird die bereits vorhandene Freigabe durch einen Vorgesetzten (wie z. B. den CEO) oder die Anweisung durch den Vorgesetzten selbst durch gefälschte E-Mails und/oder geschicktes Social Engineering per Telefonanruf vorgetäuscht. Der Vorwand für die Überweisung kann bspw. der Kauf von Unternehmensanteilen sein. Fake President kann als eine Form des Identitätsbetrugs angesehen werden. Er ist von anderen Formen wie der (i) Umleitung von Zahlungsströmen oder der (ii) Umleitung von Warenlieferungen zu unterscheiden.

Bei der Umleitung von Zahlungsströmen täuschen die Angreifer gegenüber dem angegriffenen Unternehmen eine Kommunikation mit einem bestehenden Geschäftspartner (Lieferant) vor und bitten um die Berücksichtigung einer ab sofort gültigen geänderten Kontoverbindung. Üblicherweise erfolgt die Kommunikation per E-Mail und angefügten Rechnungen. Bei der Umleitung von Warenlieferungen wird gegenüber dem angegriffenen Unternehmen die Identität eines tatsächlich existierenden Geschäftspartners (Kunde) vorgetäuscht, um Waren zu bestellen. Allerdings wird in diesem Fall um

Berücksichtigung einer geänderten Lieferadresse gebeten. Zum Teil funktioniert diese Betrugsmasche auch mit „Neukunden". Die tatsächlich existierenden Geschäftspartner (Lieferanten und Kunden), möglicherweise auch die Formate und Inhalte von offiziellen Dokumenten sowie erbrachte Leistungen sind den Angreifern demnach bekannt. Entsprechende Informationen können z. B. über gehackte E-Mail-Accounts, Social Engineering, Recherche im Internet bzw. in sozialen Netzwerken erlangt worden sein. Gemein ist allen drei Betrugsszenarien zudem, dass sie üblicherweise durch außenstehende Dritte verursacht werden. Ob und inwieweit dabei kollusives Handeln, also die aktive und bewusste Einbeziehung eines oder mehrerer Mitarbeiter eines Unternehmens in die Planung und Umsetzung der Angriffe eine Rolle spielt, ist nach wie vor schwer nachzuweisen. Die klare Unterscheidung unterschiedlicher Formen von Betrugsszenarien ist jedenfalls elementar, da sich die jeweiligen Maßnahmen zur Behandlung der Gefahren bei allen Gemeinsamkeiten auch unterscheiden können.

III. Eigenschaften eines idealtypischen Fake President-Vorfalls

Bei Fake President versucht der Angreifer die Anweisung einer betrügerischen Zahlung durch einen Mitarbeiter der Finanzabteilung oder der Buchhaltung zu erwirken. Dabei täuscht der Angreifer vor, bereits über eine Freigabe der Zahlung durch einen Geschäftsführer, das höhere Management oder auch einen juristischen Stellvertreter zu verfügen.

1. Erste Kontaktaufnahme

Die Masche beginnt häufig mit einem Anruf. Dabei stellt sich bspw. ein Anwalt einer bekannten Rechtsanwaltskanzlei vor, der die Geschäftsführung bei einer streng vertraulichen Unternehmensakquisition vertritt. Es kann aber auch der vermeintliche CEO selbst sein, der den Anruf tätigt. Oft wird zunächst betont, dass der angerufene Mitarbeiter aufgrund seiner langjährigen Treue zum Unternehmen und Integrität in dieser höchst vertraulichen Angelegenheit ausgewählt wurde. Zudem wird auf die Lösungskompetenz des Mitarbeiters angespielt. Nur er könne eine Lösung finden. Der Mitarbeiter wird nun bspw. um Überweisung eines größeren Betrages zum Erwerb von Unternehmensanteilen aufgefordert. Das Empfängerkonto befindet sich dabei regelmäßig im Ausland. Üblich sind Banken im asiatischen oder osteuropäischen Raum. Unter diesem Vorwand wird der Mitarbeiter um Identifikation einer Möglichkeit zur kurzfristigen Überweisung aufgefordert. Der Mitarbeiter wird zudem um Wahrung strengster Vertraulichkeit gebeten. Ein Bruch der Vertraulichkeit würde zudem eine Verletzung regulatorischer Anforderungen darstellen. In Einzelfällen wird hier nicht nur auf vertragliche Anforderungen, sondern auch direkt auf Aufsichtsbehörden verwiesen. Schließlich benennt der Anrufer eine weitere involvierte Person, die sich im weiteren Verlauf melden wird, da der CEO selbst und auch der aktuelle Anrufer in Verhandlungen gebunden sein würden.

Aus der ersten Kontaktaufnahme lässt sich bereits eine Fülle typischer Eigenschaften von Fake President ableiten:

- Dem Mitarbeiter wird geschmeichelt (Treue, Integrität, Kompetenz). Somit wird eine Vertrauensbasis hergestellt. Zudem wird das Bedürfnis erzeugt, die Erwartungen zu erfüllen.
- Es wird strengste Vertraulichkeit eingefordert und somit ein von außen isolierter Handlungsraum geschaffen.
- Die Angaben zur Identität sind recherchierbar und verifizierbar (z. B. die Firmierung der Kanzlei und der Name des Anwalts), wodurch das Vertrauen verstärkt und die Richtigkeit der Angaben sowie der Handlung selbst bezeugt wird.
- Die Gelder sollen in ein Land außerhalb der Einflusssphäre des überweisenden Unternehmens transferiert werden (Bank im asiatischen oder osteuropäischen Raum).
- Der Mitarbeiter befindet sich in einer hierarchisch untergeordneten Rolle, wodurch das „Recht zu Handeln" und zur Verweigerung aufgrund von Zweifeln eingeschränkt wird.
- Es wird ein Bezug zu Aufsichtsbehörden hergestellt. Die Richtigkeit der Handlung wird durch die Wirkung der Autorität verstärkt. Die Erfüllung der Pflicht gegenüber einer Autorität verstärkt die Isolation des Mitarbeiters, da er strengste Vertraulichkeit wahren muss.
- Das aufgebaute Vertrauen wird auf eine weitere Kontaktperson transferiert. Dadurch wird eine Entkopplung von der unmittelbaren Kommunikation mit dem Erstkontakt bewirkt. Die Möglichkeit der Enttarnung durch den Raum für Rückfragen wird somit reduziert.

Als Reaktion auf das Telefonat entstehen bei dem Mitarbeiter üblicherweise Zweifel. Im Extremfall können bei nicht wirksam sensibilisierten Mitarbeitern die Zweifel aber auch ausbleiben. Entscheidend ist im Zweifelsfall, ob in dieser isolierten Situation nach bestätigenden oder entkräftenden Informationen in Bezug auf die Richtigkeit der Handlung gesucht wird. Es ist davon auszugehen, dass der Großteil der Mitarbeiter, die eine regelmäßige und wirksame Sensibilisierung für diese Betrugsmasche erfahren haben, nach entkräftenden Informationen suchen wird. In der Konsequenz werden sie gegen alle Zweifel die Isolation durchbrechen und vertraute Kollegen ansprechen. Je intensiver die direkte Zusammenarbeit zwischen Vorgesetzen und Mitarbeitern im Alltag ausgeprägt ist, desto geringer ist auch die Hemmschwelle, den Vorgesetzen direkt zu kontaktieren. Ganz wesentlich an dieser Stelle ist aber die Berücksichtigung der besonderen Situation in einem Unternehmen, das Opfer eines Fake President-Angriffs wird. Oft sind es genau solche Unternehmen, in denen gerade das Management gewechselt hat und bei denen z. B. Transaktionen im asiatischen Raum oder zumindest grundsätzlich eine Expansion zur aktuellen Realität gehören. Insofern ist eine präventiv wirkende Unternehmenskultur, die eine hierarchieübergreifende Abstimmung bei Zweifelsfragen fördert, eingeschränkt. Es herrscht möglicherweise Unsicherheit in Bezug auf neue Geschäftsführer und Vorgesetzte. Die Wirksamkeit von bisherigen Sensibilisierungsmaßnahmen und somit auch die Handlungssicherheit des Mitarbeiters können eingeschränkt sein.

2. Zweite Kontaktaufnahme

In einem nächsten Schritt kann der Mitarbeiter des Unternehmens bspw. eine E-Mail mit den konkreten Überweisungsinformationen erhalten. Oft wird in diesem Zusammenhang gefragt, über welchen Weg diese Ausnahmeüberweisung am schnellsten umgesetzt werden kann und welches der maximale Überweisungsbetrag ist. Dabei wird zudem in vielen Fällen auf die Angriffstechnik des E-Mail-Spoofings zurückgegriffen. Dabei wird dem Empfänger eine vertrauenswürdige Absenderadresse vorgetäuscht.

Auch wenn latente Zweifel an der Richtigkeit der Anfrage bestehen, antwortet der Mitarbeiter bei erfolgreichen Angriffen. Dabei werden dann konkrete Möglichkeiten der Überweisung vorgeschlagen. Oft

handelt es sich dabei um nicht regelmäßig genutzte Zahlungsverfahren wie bspw. eine Anweisung der Zahlung an die Hausbank per Fax. Der Mitarbeiter teilt dabei auch mit, dass die Unterschrift eines Geschäftsführers dafür notwendig sei.

In der Regel äußert ein Mitarbeiter in den Kommunikationen an diversen Stellen seine Bedenken. Grundsätzlich findet dieser Dialog mit wenigen E-Mails innerhalb eines Tages statt. Es kann aber zwischendurch auch ein Wechsel des Kommunikationsmediums stattfinden. Die Angreifer gehen jedoch stets auf die Bedenken ein. Üblich ist z. B. eine bestätigende SMS des CEO, in der die Anfrage der Zahlung bestätigt wird. Oft wird behauptet, dass der CEO in Verhandlungen ist und daher nicht erreichbar ist. Der Angreifer (bspw. der involvierte Rechtsanwalt) bestätigt die Option der Anweisung via Fax und sendet zudem die eingescannte Unterschrift des CEO als Anlage zur E-Mail. Es wird um kurzfristige Bestätigung der Umsetzung gebeten und erneut auf die strikte Vertraulichkeit hingewiesen.

Weitere typische Eigenschaften von Fake President:

- Der betroffene Mitarbeiter selbst identifiziert den Sonderprozess auf Anfrage und eröffnet somit Handlungsoptionen.
- Technologische Angriffstechniken wie E-Mail-Spoofing können Bestandteil des Angriffsszenarios sein.
- Es können latente Zweifel bestehen, die von den Angreifern kontinuierlich adressiert werden. Es ergeben sich dadurch im Gesamtablauf aber auch Chancen zur Wirksamkeit von Gegenmaßnahmen.
- Kommunikationskanäle können innerhalb kurzer Zeit wechseln, wodurch die Entdeckungswahrscheinlichkeit des Betrugs reduziert werden soll.
- Es werden frei recherchierbare Identifikationsmerkmale (z. B. die eingescannte Unterschrift aus dem Geschäftsbericht) genutzt. Möglicherweise sind diese Informationen aber auch aus einem zuvor gehackten E-Mail-Account erlangt worden.
- Zeitdruck wird aufgebaut und aufrecht gehalten, wodurch die Möglichkeit zur Reflektion des Vorgangs eingeschränkt wird.
- Vertraulichkeit muss kontinuierlich gewahrt bleiben, wodurch die Isolation des Mitarbeiters aufrecht gehalten werden soll.

3. Anweisung der Zahlung

Unter der Voraussetzung, dass die Betrugsmasche bis zu diesem Punkt erfolgreich verläuft, erfolgt nun die Anweisung der Zahlung. Hierzu kann bspw. eine klassische Faxanweisung an die Hausbank genutzt werden. Sie enthält die Unterschriften des betroffenen Mitarbeiters und des Geschäftsführers. An dieser Stelle ergibt sich die Möglichkeit, dass eine außenstehende Partei – die Hausbank – den weiteren Erfolg des Angriffs verhindert. Sie prüft die Gültigkeit der Unterschriften und ggf. auch der Höhe des angewiesenen Betrags. Es gab aber hier Fälle, in denen Zahlungen von der Bank ausgeführt wurden, obwohl keine gültige Zeichnungsberechtigung des Geschäftsführers bestand. Das verdeutlicht das Risiko, das mit der Möglichkeit der Nutzung von Sonderprozessen verbunden ist.

Der Mitarbeiter bestätigt nun die Anweisung der Zahlung an die Hausbank gegenüber dem Angreifer. Der Angreifer selbst weist nochmals auf die strenge Vertraulichkeit hin und fügt nun sogar eine Frist hinzu. So wird in Einzelfällen für einen Zeitraum von 48-72 Stunden gefordert, mehrmals am Tag die Aufrechterhaltung der Vertraulichkeit per E-Mail zu bestätigen. Dem wird in erfolgreichen Angriffsfällen auch Folge geleistet. Für die Angreifer reduziert sich durch den Zeitraum das Risiko, dass die Zahlung doch noch aufgehalten wird. Zudem wird den Angreifern ausreichend Zeit verschafft, den empfangenen Betrag zu stückeln und auf weitere Konten zu transferieren oder auch Teilbeträge abzuheben. In einigen Fällen wird zudem versucht, weitere Zahlungen zu erwirken. Diese Vorgehensweise ist durchaus erfolgreich. Der Vorgang wird i. d. R. als Betrug erkannt, sobald der involvierte Mitarbeiter direkt oder indirekt in Kontakt mit dem tatsächlichen Geschäftsführer tritt.

Weitere typische Eigenschaften von Fake President:

- Auch wenn das Angriffsszenario innerhalb weniger Tage stattfindet, handelt es sich um einen Zeitraum, der Handlungsoptionen für Gegenmaßnahmen eröffnet.
- Die fortwährenden Zweifel des involvierten Mitarbeiters verdeutlichen, dass ein Risikoverständnis vorhanden, aber das „Recht zu Handeln“ durch geschickte psychologische und technologische Angriffstechniken ausgehebelt ist.
- Auch das überweisende Kreditinstitut ist als Bestandteil des Angriffsszenarios zu verstehen und sollte in den Handlungsspielraum zur Ergreifung von wirksamen Gegenmaßnahmen einbezogen werden.

IV. Ausgewählte Präventionsmaßnahmen

Regelmäßige Sensibilisierungs- und Schulungsmaßnahmen können die Wahrscheinlichkeit erfolgreicher Fake President-Angriffe deutlich reduzieren. Die Maßnahme sollte rollenspezifisch sein und zumindest Geschäftsführung, höheres Management und Mitarbeiter der Abteilung Finanzen und der Buchhaltung sprichwörtlich an einen Tisch bringen. Aber auch weitere Parteien, die Bestandteil üblicher Angriffsszenarien sind, können dazu eingeladen werden. Entscheidend im Rahmen der Schulungsmaßnahme ist die moderierte Diskussion – idealerweise einschließlich Rollenspiel – der psychologischen Eigenschaften eines Angriffsszenarios. Durch die unmittelbare emotionale Erfahrung wird das Problembewusstsein aller Teilnehmer geschärft und mögliche Barrieren durch Hierarchien werden abgebaut. Daneben sollte aber auch allen anderen Eigenschaften des Angriffsszenarios Raum zur Darstellung gegeben werden. Hierdurch wird insbesondere die Chance eröffnet, auch technologische Angriffstechniken wie bspw. E-Mail-Spoofing und Hacking mit den korrespondierenden Maßnahmen zur Informationssicherheit im Unternehmen in ihrer Relevanz für ähnliche Angriffsszenarien zu platzieren. Im Ergebnis sollte das Bewusstsein dafür geschärft werden, dass es sich bei Fake President um ein komplexes Angriffsszenario handeln kann, dessen Vorbereitung sich möglicherweise über einen längeren Zeitraum erstreckt.

Der Rahmen einer regelmäßigen rollenspezifischen Schulung bietet auch die Möglichkeit, einen wirksamen „Tone from the top“ zu kommunizieren. Eine klare Aussage, dass Zweifel immer mehr Gewicht haben müssen als hierarchische Barrieren, kann auch über den zwischenzeitlichen Wechsel einer Geschäftsführung hinaus Wirksamkeit entfalten. Es kann sich eine entsprechende Haltung bei den relevanten Mitarbeitern herausbilden. Damit ist eine wirksame Maßnahme gegeben, eine sowohl von Angreifern geschaffene, aber auch von einem involvierten Mitarbeiter gefühlte Isolation zu durchbrechen. Awareness-Maßnahmen wie News Flashs, Posts oder klassische Poster auf den Fluren eines Unternehmens können das Grundverständnis für die Gefahr von Fake President für das gesamte Personal ergänzend fördern. Die Ausstrahlungswirkung dieser Maßnahme auf die Mitarbeiter der Abteilung Finanzen und der Buchhaltung sollte

nicht unterschätzt werden. Sie betont die besondere Verantwortung dieser Mitarbeiter in Bezug auf die Betrugsmasche und bietet zudem das Potenzial, auch Wirksamkeit in Bezug auf ähnliche Betrugsszenarien, die wiederum einen breiteren Mitarbeiterkreis treffen können, zu entfalten.

Regelmäßigkeit von Schulung und Sensibilisierung beinhaltet zudem die gezielte Berücksichtigung neuer Mitarbeiter, Manager oder Geschäftsführer, da gerade Unternehmen mit Veränderungen in relevanten Funktionen Ziele von Angreifern sind. Auch die Erweiterung von Rollen- und Tätigkeitsprofilen im Unternehmen, branchenübliche Betrugsmuster zu kennen bzw. zu erkennen, kann bereits eine notwendige und wirksame Maßnahme sein.

Ergänzend sind die folgenden Maßnahmen geeignet, die Kontrolle über Zahlungsprozesse zu erhöhen:

- Zentralisierung und Harmonisierung des Zahlungsverkehrs,
- Reduktion von Bankkonten,
- Transparenz über Konten sowie Berechtigungen,
- Limitierung von Zahlungsberechtigungen,
- Verminderung bzw. Abschaffung von (manuellen) Sonderprozessen.

Im Wesentlichen wird dadurch der Handlungsspielraum eines involvierten Mitarbeiters deutlich eingegrenzt, sodass auch bei erfolgreichen psychologischen Fertigkeiten der Angreifer nur noch eingeschränkte oder gar keine prozessualen Möglichkeiten für eine erfolgreiche Überweisung bestehen. Insbesondere schaffen die Zentralisierung des Zahlungsverkehrs und die Abschaffung von Sonderprozessen die Möglichkeit, verlässlichere Techniken der Authentifizierung zu implementieren, sodass die Nutzung einer leichter zu erlangenden digitalisierten Unterschrift für einen Angriff nicht möglich ist. Zusätzlich ermöglichen die genannten Maßnahmen ein gezieltes und automatisiertes Monitoring auffälliger Zahlungen. Entsteht daraus eine erfolgreiche Detektion einer auffälligen Zahlungsanweisung, so kann auch diese Maßnahme geeignet sein, die Isolation eines involvierten Mitarbeiters zu durchbrechen und rechtzeitig sicherheitsrelevante Mitarbeiter einzubeziehen. Gerade da die psychologischen Angriffspraktiken sehr ausgefeilt sein können und modifiziert werden, kommt den beschriebenen komplementären Maßnahmen eine hohe Bedeutung zu.

Eine wesentliche Eigenschaft von ausgefeiltem Fake President ist jedoch, dass gerade etablierte Zahlungsfreigabe und –anweisungsverfahren unter Berücksichtigung von Unternehmensvorgaben genutzt werden – allerdings unter Vortäuschung einer Freigabe durch einen Vorgesetzten.

Es darf nicht außer Acht gelassen werden, dass bei einem idealtypischen Fake President-Angriff ein unwissender Mitarbeiter ausgespielt wird. Das Szenario ändert sich, sobald ein wissender Mitarbeiter – also kollusives Handeln – in die Betrachtung einbezogen wird. Bei der Aussicht auf hohe zweistellige Millionenbeträge kann der intensive Planungs- und Umsetzungsaufwand aus der Perspektive der Organisierten Kriminalität ökonomisch durchaus sinnvoll sein, auch wenn sich das Angriffsmuster dann von einem trivial umgesetzten Massenphänomen zu einer länger geplanten und komplexen Einzeltat wandelt.

Die Vorbereitung der Reaktion im Ernstfall sollte daher Bestandteil einer ausgewogenen Prävention sein. Hierdurch werden die Grundlagen für unmittelbares Handeln geschaffen. Dabei sind die folgenden wesentlichen Maßnahmen empfehlenswert:

1. Etablierung geschulter Kontakte und regelmäßiges Update der Kontakte: a) die Hausbank, b) Schwerpunktdezernate der inländischen Strafverfolgungsbehörden, c) ausländische Strafverfolgungsbehörden zumindest in Ländern und Regionen der Geschäftserbringung, d) spezialisierte Kanzleien für Wirtschaftsstrafrecht in den vorgenannten Ländern und Regionen, da diese durch Kenntnis der lokalen Gegebenheiten zur wirksamen Erstreaktion beitragen können sowie e) inländische Spezialisten für die Beweissicherung und unabhängige Sachverhaltsaufarbeitung mit einem internationalen Netzwerk an den relevanten Orten der Geschäftserbringung eines Unternehmens.
2. Implementierung von Prozessen und Verfahren, die eine kurzfristige Sicherung von Beweisdaten wie z. B. Kommunikationsdaten und übliche Office-Dateien auf Servern, Laptops, Tablets, Mobiltelefonen, Telefonanlagen für definierte Zwecke ermöglichen. Die Prozesse und Verfahren sollten den besonderen Anforderungen bspw. in Bezug auf Datenschutz, Telekommunikationsgesetz und Mitbestimmung genügen.
3. Erstellung eines Leitfadens bzw. Protokolls zum Umgang mit Mitarbeitern und Vorgesetzten, die in den Vorfall involviert sind. Insbesondere ist hierbei die Verhinderung der möglichen Löschung oder Manipulation von Beweisdaten zu regeln.

Die entsprechend des Risikos der Geschäftstätigkeit zu gestaltenden Maßnahmen erhöhen nicht nur die Reaktionsgeschwindigkeit, sondern sind auch geeignet, die Verwertbarkeit der Ergebnisse der Beweissicherung und Aufarbeitung eines Vorfalls im juristischen Nachgang zu gewährleisten.

V. Empfohlene Reaktionsmaßnahmen im Ernstfall

Die zuvor skizzierte Vorbereitung der Reaktion im Ernstfall gibt bereits den Rahmen der Ablaufprozedur vor. Die schnellstmögliche Umsetzung der folgenden Schritte ist zu empfehlen:

1. Die überweisende Bank ist zu kontaktieren. Der Zahlungslauf ist möglicherweise noch nicht umgesetzt, da noch eine manuelle Prüfung der Zahlungsanweisung durch die Bank erfolgt oder die Zahlungsanweisung sich noch in der systemseitigen Verarbeitung befindet.
2. Die empfangende Bank, die Strafverfolgungsbehörde sowie ggf. eine Kanzlei im Empfängerland ist zu kontaktieren. Auch die empfangende Bank muss eingebunden werden, da sie die Möglichkeit hat, Einfluss auf die Weiterleitung einer empfangenen Zahlung zu nehmen. Ziel der Angreifer ist es, die Zahlung zu stückeln und auf andere Konten weiterzuleiten oder Teilbeträge abzuheben. Lokale Strafverfolgungsbehörden haben ggf. die Möglichkeit, Konten einzufrieren bzw. Zahlungen nachzuverfolgen. Lokale Kanzleien können durch die Kenntnis der örtlichen Gegebenheiten möglicherweise bei der Umsetzung notwendiger Schritte unterstützen.
3. Es sollte Strafanzeige im Inland erstattet werden.
4. Entsprechend der Situation und Verfügbarkeit unternehmenseigener Kapazitäten und Fertigkeiten sollten Spezialisten für die Beweissicherung und Sachverhaltsaufarbeitung eingebunden werden.
5. Das Protokoll zur Behandlung von Mitarbeitern und Vorgesetzten, die in den Vorfall involviert sind, sollte genutzt sowie Beweisdaten gesichert werden.
6. Die Abteilung Finanzen, die Buchhaltung sowie relevante Gesellschaften in der Unternehmensgruppe sollten kurzfristig informiert und sensibilisiert werden. Erhöhte Wachsamkeit und Monitoring

relevanter Geschäftsprozesse ist geboten. Der Hintergrund hierfür ist die Möglichkeit, dass zeitgleich oder mit leichtem Versatz Angriffe auf weitere Unternehmensgesellschaften oder sogar dieselbe Gesellschaft stattfinden. Je nach individueller Gestaltung des Angriffsszenarios kann die Einbeziehung relevanter Geschäftspartner erwogen werden.

7. Der Vorfall sollte aufgearbeitet und ggf. die juristische Nachverfolgung eingeleitet werden. Es sollte eine Überleitung in die Remediation stattfinden.

VI. Fazit

Fake President ist gekommen, um zu bleiben. Der Grund dafür ist einfach oder eben auch so komplex wie die menschliche Psychologie. Eine umfassende und ursachenorientierte Risikobeurteilung und Maßnahmenableitung ermöglicht zwar eine wirksame Eingrenzung der Gefahr für ein Unternehmen, Opfer eines Fake President-Betrugs zu werden. Insbesondere der Erfolg trivialer und noch immer erfolgreicher Angriffsszenarien über erkennbare Spoofing-E-Mails und anschließende Überweisung unter Missachtung von klaren Unternehmensrichtlinien können verhindert werden. Fehlverhalten in diesen Fällen sollte auch eine Sanktionierung erfahren, um ein wirksames Kontrollumfeld zu schaffen. Doch solange Zahlungsprozesse nicht ausnahmslos vollautomatisiert in einem Unternehmen durchgeführt werden, bleibt die Eingriffsmöglichkeit über die Beeinflussung von Mitarbeitern ein latentes Risiko. Doch selbst unter dieser Voraussetzung werden strategische Betrüger den Angriffspunkt verschieben und sich auf die auslösenden Ereignisse automatischer Zahlungsprozesse und die dahinter stehenden Personen fokussieren. Alternativ könnte sich der Schwerpunkt der Angreifer auch auf kollusive Strategien verlagern. Ein Social Engineering-Angriff ist in der Summe aller Eigenschaften eben nicht trivial. Insbesondere nicht in Kombination mit einem dynamischen und innovativen technologischen Umfeld. Er ist nicht gänzlich und auf Dauer vermeidbar. Daher kann der professionelle Umgang mit solcher Art Gefahren und den involvierten Mitarbeitern sogar einen Wettbewerbsvorteil für Unternehmen darstellen. In einer von Innovation, Technologie und Menschlichkeit geprägten Wertschöpfungskette sind die Kompetenzanforderungen an jeden einzelnen Mitarbeiter und das Management sehr hoch. Dennoch spricht eine Kultur des Lernens aus kritischen Situationen eine deutliche und nachhaltige Sprache. Solche Unternehmen werden langfristig die kompetentesten Mitarbeiter rekrutieren und halten, Gefahren wirksam reduzieren und den Erfolg des Unternehmens nachhaltig im Mittelpunkt stehen lassen.

AUTOR

Thomas Fritzsche *ist Director im Bereich Financial Advisory beim Prüfungs- und Beratungsunternehmen Deloitte. Mit seinem Schwerpunkt auf Forensic Technology verantwortet er vorrangig analytisch und technologisch geprägte Projekte zur Beantwortung von Fragestellungen an große und heterogene Daten- und Dokumentenmengen im Rahmen von Litigations, Investigations sowie Mergers & Akquisitions. Er ist Autor von Publikationen zu Computerkriminalität und Cyber-Risiken sowie Dozent am Zentrum für Weiterbildung und Wissenstransfer an der Universität Augsburg.*

Abbildung: Fake President Fraud