CEO Fraud, Phishing und Social Engineering

Schutz vor Cyberkriminalität

Eine Zahlungsaufforderung per E-Mail vom vermeintlichen Chef kurz vor Arbeitsende … und schon ist der grosse finanzielle Verlust leider Realität. Im Beitrag wird gezeigt, mit welchen Tricks Cyberkriminelle Mitarbeitende zu manipulieren versuchen und wie Unternehmen sich dagegen schützen können.

Von Chris Eckert

Geldüberweisung unter Zeitdruck

Der Geschäftsführer eines 16-köpfigen Start-up-Unternehmens in der Softwareentwicklung befindet sich gerade für mehrere Tage im Tessin im vorgezogenen Weekend. Seine Assistentin, die gewissermassen auch seine rechte Hand ist, möchte an diesem Freitag ausnahmsweise etwas früher Feierabend machen und tätigt die letzten administrativen Arbeiten. Kurz nach 15 Uhr erhält sie von ihrem Chef per Mail die Aufforderung, dass bis spätestens um 15.30 Uhr CHF 25 000.– als Anzahlung für eine zusätzliche Softwarelösung eines Zulieferers auf ein Bankkonto in Italien zu überweisen sei. Wenn das Geld nicht rechtzeitig überwiesen werde, platze der einmalig günstige Deal, und bereits in der darauffolgenden Woche sei das gleiche Angebot ein paar Tausend Franken teurer. Die Angestellte weiss, dass ihr Chef oft in seiner Freizeit spontan Geschäftspartner im In- und Ausland trifft, verzichtet darum auf Rückfragen und zahlt das Geld via E-Banking ein. Letztlich hat sie die Kompetenz zur Auslösung der Zahlung für solche Beträge, und es ist bereits 15.20 Uhr. Ausserdem steht sie unter Zeitdruck und wollte das Büro eigentlich schon längst verlassen, da ihr Freund draussen im Auto auf sie wartet. Und schliesslich ist sie eine zuverlässige Person, die bisher jeden Auftrag des Chefs pflichtbewusst erledigt hat.

Dass dies ein fataler Fehler war, stellt sich am Montagmorgen heraus. Tatsächlich war es nicht der Geschäftsführer, sondern ein unbekannter Internet-Betrüger, der die Mail geschickt und sie dazu gebracht hat, die Überweisung zu tätigen. Der Schaden lässt sich nicht mehr beheben, eine Strafanzeige bei der Polizei bringt kaum etwas, und die Spur zum Konto in Italien lässt sich – wenn überhaupt – nur langwierig ermitteln. An die überwiesene Geldsumme kommt man nicht mehr. Wie sich Tage später herausstellt, wurde der Betrag bereits abgehoben und das Konto aufgelöst.

Kleinste Nachlässigkeiten in der IT oder bei der elektronischen Kommunikation können von Cyberkriminellen ausgenützt werden.

Modus operandi (Tatvorgehen)

Cyberattacken in mannigfaltigen Varianten bedrohen die Unternehmen und Institutionen in der Schweiz immer häufiger. Leider muss man sich nicht mehr die Frage stellen, OB, sondern WANN man angegriffen, gehackt oder betrogen wird. Heute ist es auch völlig unbedeutend, ob es sich beim Geschädigten um einen kleinen Familienbetrieb, eine systemrelevante Institution oder um einen internationalen Konzern handelt. Kleinste Nachlässigkeiten in der IT, Versäumnisse bei der Informationssicherheit, ein Manko in der Organisation und den Prozessen oder ungenügende Awareness der Mitarbeitenden werden von Hackern oder sonstigen Cyberkriminellen gnadenlos ausgenutzt.

Mit raffinierten Methoden erzeugen Kriminelle Hektik, Druck und bisweilen auch Angst, welche die Mitarbeitenden aller Stufen zu einer Vielzahl von Fehlern verleiten können. Nachlässigkeiten, gutgläubiges sowie unkritisches Denken und Verhalten werden nicht nur bei der Industrie- und Wirtschafsspionage ausgenutzt, sondern sind leider bestens geeignet zur schnellen und anonymen monetären Bereicherung.

Beim «CEO-Fraud», auch «Fake President Trick» oder allgemein auch als Variante «Phishing Mail» bekannt, handelt es sich um eine Betrugsmasche, bei der sich Cyberkriminelle meist als Chef eines Unternehmens ausgeben und ihre Opfer in fingierten E-Mails dazu auffordern, hohe Geldsummen ins Ausland zu überweisen. Meist wird von einer dringlichen, vertraulich zu behandelnden Transaktion gesprochen, um zusätzlichen Druck bei den Adressaten aufzubauen.

Die Unbekannten erlangen vorgängig mittels Social-Engineering-Methoden alle erforderlichen Informationen über die Firma und ihre wichtigsten Mitarbeitenden. Danach adressieren sie sehr gezielt jene Angestellten, die Zugang zu sensiblen Daten haben oder berechtigt sind für Zahlungstransfers.

Gegenmassnahmen

Wir sind dieser Bedrohung nicht einfach schutzlos ausgesetzt. Es gibt einige Gegen- und Präventionsmassnahmen, vor allem im Bereich der Awareness, welche hochwirksam sind und mit wenig Aufwand implementiert werden können. Es lohnt sich z.B. in jedem Fall, in Ihrem Betrieb alle Verantwortlichen zu instruieren und im Rahmen einer Awarenesskampagne einen Leitfaden oder eine Handlungsanweisung zu dieser Thematik zu erarbeiten (lassen).

Allgemeine Massnahmen im Umgang mit verdächtigen Mails

- Bei Erhalt eines entsprechenden E-Mails mit einer ungewöhnlichen Zahlungsanweisung sollte in jedem Fall der Inhalt der Nachricht kritisch geprüft werden (u.a. auf Schreibfehler und Schreibstil achten), bevor eine Überweisung ausgelöst wird.
- Überprüfen der E-Mails auf Plausibilität des Inhalts und korrekte Absenderadresse, z.B.:
  max.muster@swissbp.ch
  = unbedenklich
  max.muster@gmail.com
  = kritisch/evtl. gefälscht
  Grundsätzlich sollten Sie immer hellhörig werden, wenn Ihnen nahestehende Personen aus der Firma Sie statt wie üblich vom geschäftlichen Account über eine private oder unbekannte Mailadresse kontaktieren oder Ihnen Aufträge erteilen.
- Sofortiges Verifizieren der Zahlungsaufforderung mittels telefonischen Rückrufs bzw. persönlicher Kontaktnahme bei der auftraggebenden Person.
- Bei anhaltender Unsicherheit sofortige Rücksprache mit dem direkten oder einem anderen Vorgesetzten.
- Im absoluten Zweifelsfall lieber einmal mehr prüfen, statt möglichst schnell der Anweisung nachzukommen.
- Dringendste Massnahme, falls die Summe bereits überwiesen wurde: Sofort mit dem direkten Vorgesetzten und dem Zuständigen der Sicherheit, wenn nötig auch ausserhalb der Bürozeiten, Kontakt aufnehmen. Es gibt Möglichkeiten – sofern der Fehler schnell entdeckt wurde – mit dem entsprechenden Bankinstitut in Kontakt zu treten und die Überweisung an die ausländische Empfängerbank zu verhindern. Der Zeitfaktor spielt hier eine grosse Rolle!
- Rücksprache mit der internen Stelle, um ggf. eine Strafanzeige bei der zuständigen Polizeidienststelle auszulösen.

Awareness für alle Mitarbeitenden

- Achten Sie darauf, welche Informationen und Daten über Sie und Ihre Firma öffentlich sind bzw. wo und was Sie und Ihre Mitarbeitenden im Zusammenhang mit Ihrem Unternehmen publizieren.
- Vermeiden Sie auch, scheinbar unwichtige Dinge über Ihren Berufsalltag in den sozialen Medien zu posten (z.B. Facebook, Instagram etc.).
- Führen Sie klare Abwesenheitsregelungen und interne Kontrollmechanismen (z.B. Vieraugenprinzip bei Geldtransaktionen) ein.
- Sensibilisierung ist alles. Nutzen Sie die Awareness-Angebote für Ihre persönliche, berufliche und private Sicherheit: Schwachstelle Mensch, Informations- und Datenschutz, Betrugsphänomene, Social Engineering etc.

Mehr Auskünfte und gezielte Schulungen erteilt Ihnen gerne: www.swissbp.ch.

Chris Eckert ist Founding Partner der Swiss Business Protection AG. Er verfügt über mehr als 30 Jahre kriminalistische Erfahrung, erworben bei der Kantonspolizei Zürich sowie der Bundeskriminalpolizei. Seit über 12 Jahren ist er selbstständig. Als Kriminalist, CSO/CISO a.i. in den Bereichen Informationssicherheit, Forensik und Kriminalprävention stellt er seine Erfahrung konzeptionell, strategisch und operativ zur Verfügung. Daneben ist er als Dozent in den Fachbereichen Social Engineering, Informationssicherheit und Wirtschaftsschutz tätig.

Datenschutz?

Kennen Sie das? Sie rufen irgendeine Servicenummer an oder erhalten einen Anruf von einer solchen Nummer. Sie fragen nach genaueren Informationen, und dann heisst es: «Aus datenschutzrechtlichen Gründen können wir keine weitere Information geben.» Und weil Sie Datenschutz ohnehin reichlich nervig finden und sich deshalb nie vertieft damit auseinandergesetzt haben – nur schon diese Cookie-Zustimmungen auf den Websites die ganze Zeit! –, akzeptieren Sie diese Begründung, ohne sie zu hinterfragen. Damit hat Ihr Gesprächspartner sein Ziel erreicht: Kein Einblick in die eigenen Karten. Mit der Nebelpetarde «Datenschutz» fast immer möglich. Die grosse Blackbox, immer als Entschuldigung gut, weil (fast) niemand den Durchblick hat.

Aber nein. Lassen Sie sich nicht gängeln. Nicht immer, wenn der sog. Datenschutz bemüht wird, geht es auch wirklich um Datenschutz. Als Orientierungspunkt diene Ihnen die Information, dass der Datenschutz nur den Schutz von Personendaten im Visier hat. Personendaten sind alle Angaben, die sich auf bestimmte oder bestimmbare Personen beziehen. Eine weite Definition, wenn man berücksichtigt, dass selbst IP-Adressen als solche qualifiziert werden (weil Rückschlüsse auf deren Benutzer möglich sind). Nichtsdestotrotz dürfen Sie die Personenbezogenheit von gewissen Informationen, die Ihnen verweigert werden, infrage stellen. Z.B., wenn Ihnen die Auskunft verweigert wird, wie viel Benzin ein Auto denn normalerweise braucht.

Allerdings nützt es möglicherweise wenig, wenn Sie sich nicht abspeisen lassen. Denn die Datenschutzkeule wirkt meistens auf beide Seiten einschüchternd. So ist wohl auch die Person am Telefon nicht in der Lage, ein qualifiziertes Gespräch darüber zu führen, ob es hier tatsächlich um schützenswerte Personendaten geht. Wenn Sie aber merken, dass es beim Anrufer zu Stolperern im sonst eingeschliffenen Text kommt, dann wissen Sie, dass der Blocker «Datenschutz» wohl ganz bewusst auf dem Skript steht. Weil es irgendjemandem nützt, wenn Sie nicht die Infos bekommen, die Sie angefragt haben.

Astrid Lienhart ist Fachanwältin SAV Arbeitsrecht und als Rechtsanwältin in der Kanzlei Rechtskraft sowie als Head Legal eines Deep-Tech-Startups in Zürich tätig.