SANS SECURITY AWARENESS

OUCH!

Der monatliche Security Awareness Newsletter für Jedermann

CEO Betrug / BEC

Was ist CEO Fraud / BEC?

Cyber-Angreifer arbeiten kontinuierlich daran eine E-Mail-Angriffsform namens CEO Fraud oder Business Email Compromise (BEC) zu verbessern. Dabei handelt es sich um gezielte E-Mail-Angriffe, die ihr Opfer dazu verleiten, eine Aktion durchzuführen, die es nicht durchführen sollte. In den meisten Fällen sind die Angreifer hinter Geld her. Die Cyber-Angreifer spähen ihre Opfer vor dem Angriff bis ins kleinste Detail aus, weshalb diese Art Angriff so gefährlich ist. Außerdem ist es für Sicherheitstechnologien sehr schwierig, diese Angriffe zu stoppen, da es keine infizierten E-Mail-Anhänge oder bösartige Links zu erkennen gibt. Der Angriff funktioniert wie folgt:

Der Cyber-Angreifer späht über das Internet das ins Visier genommene Opfer aus und sucht anschließend Personen, mit denen es häufig interagiert. Hat der Angreifer es zum Beispiel auf Sie abgesehen, würde er versuchen herauszufinden wer Ihr Vorgesetzter ist oder mit wem Sie gerade Geschäfte machen. Der Cyber-Angreifer erstellt dann eine E-Mail, gibt darin vor, eine dieser Personen zu sein und sendet die E-Mail an Sie. Er behauptet, das Anliegen sei dringend und macht ihnen vor, dass Sie sofort etwas unternehmen müssen, z. B. bei einer Rechnung den Zahlungsempfänger ändern, oder ihm sensible Dokumenten zukommen zu lassen. Die E-Mail funktioniert, indem sie Sie dazu bringt, das zu tun, was die Angreifer wollen. Hier sind zwei Beispiele, wie ein solcher Angriff funktionieren könnte.

Banküberweisung: Ein Cyberkrimineller ist hinter Geld her. Er kundschaftet das Unternehmen aus, für das Sie arbeiten, z.B. wer in der Kreditorenbuchhaltung arbeitet oder wer für den Geldtransfer verantwortlich ist. Der Kriminelle erstellt und sendet dann eine E-Mail an diese Personen, die vorgibt, von ihrem Chef oder einem leitenden Angestellten zu sein. Die E-Mail teilt ihnen mit, dass ein Notfall vorliegt und das Geld sofort auf ein neues Bankkonto überwiesen werden muss. Die E-Mail zwingt sie dazu, einen Fehler zu machen, und in Wirklichkeit schicken sie Geld an den Cyberkriminellen.

Steuerbetrug: Cyberkriminelle sind hinter persönlichen Informationen her, die sie für Steuerbetrug verwenden können. Einer der schnellsten Wege dies zu erreichen ist, die Informationen aller Mitarbeiter eines Unternehmens zu stehlen. Die Cyberkriminellen recherchieren und identifizieren, wer in der Personalabteilung arbeitet. Sie senden dann gefälschte E-Mails an diese Personen und geben vor, ein leitender Angestellter oder vielleicht jemand von der Rechtsabteilung zu sein. Der Inhalt der E-Mails erzeugt eine dringende Situation, nämlich das die Steuerinformationen über alle Mitarbeiter sofort eingereicht werden müssen. Die Mitarbeiter in der Personalabteilung denken, dass sie die sensiblen Dokumente an die Führungskraft schicken, während sie sie in Wirklichkeit an Cyberkriminelle senden.

Wie können Sie sich schützen

Was können Sie also tun, um sich zu schützen? Der gesunde Menschenverstand ist Ihre beste Verteidigung. Hier sind die gängigsten Hinweise nach denen Sie suchen müssen.

Die E-Mail ist sehr kurz und dringend (oft nur ein paar Sätze) und die Signatur besagt, dass die E-Mail von einem mobilen Gerät gesendet wurde.

Es wird ein starkes Gefühl der Dringlichkeit erzeugt, das Sie dazu drängt, die Richtlinien Ihres Arbeitgebers zu ignorieren oder zu umgehen. Befolgen Sie immer arbeitsbezogene Richtlinien und Verfahren, auch wenn die E-Mail von Ihrem Chef oder sogar vom CEO zu kommen scheint.

Die E-Mail ist arbeitsbezogen, verwendet aber eine private E-Mail-Adresse wie @gmail.com oder @hotmail.com.

Die E-Mail scheint von einem leitenden Angestellten, Mitarbeiter oder Anbieter zu stammen, den Sie kennen oder mit dem Sie arbeiten, aber der Ton der Nachricht klingt nicht nach ihnen.

Es werden Zahlungsanweisungen bereitgestellt, die sich von denen unterscheiden, die Sie bereits erhalten haben, z.B. die sofortige Zahlung auf ein anderes Bankkonto.

Wenn Sie den Verdacht haben, dass Sie beruflich ins Visier genommen wurden, stoppen Sie alle Interaktionen mit dem Angreifer und melden Sie dies Ihrem Vorgesetzten. Wenn Sie zu Hause in eine solche Situation gelangen und vielleicht sogar eine Überweisung vorgenommen haben, melden Sie dies sofort Ihrer Bank und dann den Strafverfolgungsbehörden.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT Sicherheit spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Gast-Autor

Don Cavender *ist ein ehemaliger Special Agent des FBI mit über 22 Jahren Erfahrung in digitaler Forensik und Cyberkriminalität. Zuletzt war er als BEC-Koordinator in Washington DC für Cyberkriminalität zuständig. Er lehrt und forscht in den Bereichen Digitale Forensik und Cyber-Ermittlungen.* @don_cavender https://www.linkedin.com/in/donald-cavender

Ressourcen

Social Engineering:	https://www.sans.org/u/HE3
Stopp den Phishzug:	https://www.sans.org/u/HE8
Stoppen Sie Malware:	https://www.sans.org/u/HEd
Schutz Ihrer Anmeldeinformationen:	https://www.sans.org/u/HEi