Phishing-Awareness Spezialisten: Hüter des Vertrauens in einer digitalen Welt

Geschrieben von Joshua Bucheli, KI-Ethik Forscher und Fellow beim ForHumanity Center, in Zusammenarbeit mit IT-Security Manager Kai Dorner und Peter Kosel, Gründer von cyberunity

Illustration from Insta: the_doodling_crow

In den letzten Jahren haben YouTuber wie kitboga und Jim Browning eine Online-Faszination für 'Scambaiting' – die Aufdeckung von Callcenter-Betrug – geweckt. Diese Cyber-Bürgerwehr gibt sich als gefährdete IT-Nutzer aus, um als IT-Support getarnte Phishing-Betrüger zu ködern. Die vermeintlichen Kunden drehen somit den Spiess um, lassen die Betrüger auffliegen und erreichen damit Millionen von Zuschauern.

Diese Viral-Videos sind zwar komisch, aber nicht zum Lachen - sie zeigen, wie leicht man auf Phishing-Betrügereien hereinfallen kann, und sie verdeutlichen, wie wichtig es ist, das Bewusstsein dafür zu schärfen, wie man vertrauenswürdige Parteien erkennt.

Vertrauen ist der Grundstein, auf dem alle unsere sozialen und auch digitalen Interaktionen basieren. Wir vertrauen dem E-Banking mit unseren Finanzen, Apps mit unseren Passwörtern, Systemen mit unseren Infrastrukturen und Clouds mit unseren Daten. Phishing-Angriffe sind eine Form des Social Engineering, die dieses Vertrauen ausnutzt und damit eine der grössten Bedrohungen für die Datensicherheit darstellt.

Wo steht das Thema Phishing heute?

Im Gegensatz zu technischen Cyberangriffen, bei denen Verschlüsselungen mit Brute-Force-Ansätzen geknackt oder Exploits zur Ausnützung von Schwachstellen verwendet werden, ist Phishing eine subtilere Angelegenheit. Es funktioniert nach dem gleichen Grundsatz wie das gewöhnliche Angeln: man wirft köder aus und schaut wer anbeisst. Das Ziel ist es, Benutzerdaten oder Zugriff auf Systeme zu ergaunern, indem eine legitime Website imitiert wird. Da es auf dem einfachen Prinzip der Täuschung beruht, ist es zu einem Hauptbestandteil des Arsenals von Cyber-Kriminellen geworden.

«Hacker locken Benutzer entweder mittels Links auf eine gefälschte Anmeldeseite um dort ihre sensiblen Daten einzugeben oder verleiten sie zum Herunterladen von Malware oder Ransomware auf ihre Geräte. Solche Angriffe können den Hackern nicht nur Zugang zu einem System oder sensiblen Daten verschaffen, sondern sie können auch jemanden von diesen Systemen und Dateien aussperren, bis ein Lösegeld gezahlt wird.» - erklärt IT-Security Manager, Kai Dorner.

Was Phishing unter den Cyberangriffen einzigartig macht, ist die Tatsache, dass es sich auf Social Engineering - die Manipulation der Sozialpsychologie - stützt, um Menschen auszunutzen.

Wer sich für mehr Details zum Thema Social Engineering interessiert, ist eingeladen, sich Kai's Anti-Phishing-Modell anzusehen, die sechs Prinzipien der Überredung auf den Seiten 8-10 seiner Masterarbeit nachzulesen oder hier mehr über die Feinheiten des ‘Hackens von Menschen’ zu erfahren.

Wohin bewegt sich das Thema Phishing?

Wie der Komiker und Regisseur Jordan Peele mit seinem Obama-Deepfake zeigt, führt das Aufkommen immer fortschrittlicherer Technologien zur Gesichts- und Stimmerkennung dazu, dass die Raffinesse von Phishing-Angriffen neue Dimensionen erreicht. Mit dem Fortschritt dieser Technologien wird die Beurteilung der Vertrauenswürdigkeit von Materialien immer schwieriger, was ‘Vishing’ (Voice-Phishing) und andere Varianten des Phishings umso gefährlicher macht.

Die Unternehmen beginnen zu erkennen, dass solche Probleme ihrer Aufmerksamkeit bedürfen. Es gibt jedoch einen Unterschied zwischen Wissen und Bewusstsein, und insgesamt ist das Bewusstsein dafür, was Phishing mit sich bringt, immer noch begrenzt - das leichtfertige Gefühl “Warum sollte sich jemand für mich interessieren?” erweist sich immer noch als allzu weit verbreitet.

Während einige Branchen, vor allem der Finanzsektor, bei der Implementierung von Anti-Phishing-Strategien die Nase vorn haben, müssen die meisten Unternehmen noch erkennen,

welchen Wert selbst kleine Schritte wie Mitarbeiter-Workshops oder Mini-Sensibilisierungskampagnen für ihre Image- und Jobsicherheit haben, betont Kai.

«Es wird noch viel zu oft weggeschaut, und das ist das Schlimmste, was ein Unternehmen in der heutigen Zeit tun kann. Selbst etwas so Einfaches wie das Thema bei einem Kaffee mit den Mitarbeitenden anzusprechen, kann lohnende Ergebnisse bringen - schliesslich kann ein partizipativer Gedankenaustausch effektiver sein, als sich ausschliesslich auf webbasiertes Training zu stützen.»

Phishing-Awareness Spezialisten – Gefragte Fähigkeiten und Ausbildungen

Phishing-Angriffe missbrauchen das Vertrauen - der Schutz vor solchen Angriffen wird daher in erster Linie eine Frage der Bewusstseinsbildung sein. Unternehmen werden zunehmend CISOs, ISOs und Operational Risk Officers brauchen, die ihnen helfen, zwischen legitimen und böswilligen Drittparteien zu unterscheiden, und die im Sinne des IUS auch ihre Mitarbeitenden darin schulen können.

Dies erfordert Cybersecurity-Anwärter:innen mit soliden analytischen Fähigkeiten, einer breiten Palette an IT-, Cybersecurity- und Betrugserkennungs-Know-How sowie das Talent, diese Fähigkeiten an die Mitarbeitenden zu vermitteln.

«Arbeitgeber sind auf gut ausgebildete Mitarbeitende angewiesen, die verstehen, wie Server aufgebaut, betrieben und unterhalten werden, wie Mail-Filter Nachrichten als Phishing detektieren sowie solide Grundlagen in Netzwerktechnik, Cloud- und Systemarchitektur besitzen», erzählt Kai.

Je grösser das Unternehmen ist, desto höher ist die Wahrscheinlichkeit, dass es diese Themen auf einer umfassenderen Inhouse-Basis bearbeiten möchte. Für diejenigen, die sich für solche Positionen interessieren, sind Grosskonzerne eine gute Anlaufstelle. In den meisten anderen Fällen ist Consulting angesagt, wobei spezialisierte Security-Beratungen fachbezogene Positionen in verschiedenen Nischen der Phishing-Awareness und -Sicherheit anbieten.

Praktische Erfahrung in der Implementierung von Phishing-bezogenen Cybersecurity-Massnahmen wie Multi-Faktor-Authentifizierung, VPN- und Proxy-Dienste, Firewalls, Datenverschlüsselung, das Einstellen von Filtern sowie die Durchführung von Schwachstellenanalysen und Penetrationstests sind weitere Fähigkeiten, die Phishing-Awareness Spezialisten in ihren Bewerbungen hervorheben sollten.

In Bezug auf Zertifikate ist jede professionelle Ausbildung, die Kenntnisse in den Bereichen Betrugserkennung, Ethical Hacking oder Cybersicherheit im Allgemeinen nachweist, wie z. B. CISSP, CISM, CCAP, CEH und die PhishMe-Zertifizierung von Cofense, von Vorteil.

Vertrautheit mit internationalen Implementierungsstandards und Richtlinien wie den NIST-Frameworks, dem BSI IT-Grundschutz-Kompendium, dem COBIT-Framework der ISACA, dem

(ISC)^2 Body of Knowledge, dem MITRE ATT&CK Enterprise-Framework oder dem ISO/IEC 27001 ist ebenfalls ein Plus.

Kai betont jedoch, dass praktische Erfahrungen weitaus wertvoller sind als jedes Zertifikat – «die Türen zu einer Karriere im Bereich Phishing-Awareness stehen praktisch jedem offen, der eine Leidenschaft und einschlägige Erfahrung nachweisen kann».

Persönlichkeit – über technisches Know-How hinaus:

Wie bei den meisten anderen Karrierewegen in der Cybersicherheit sind Hard-Skills nicht die einzigen Zutaten im Erfolgsrezept. Es bedarf einer besonderen Art von Persönlichkeit, um ein effektiver Phishing-Awareness Spezialist zu sein.

Unternehmen brauchen hochgradig soziale 'Awareness-Typen' mit einem Händchen für die Verbreitung von Botschaften - Teamplayer mit der nötigen Neugier, Geduld und Kommunikationsfähigkeit, um mit Konfliktfällen produktiv umzugehen. Idealerweise bringen diese Kandidaten auch Gewohnheiten mit, die denen von Sicherheitsscouts ähnlich sind - ein Bestreben, ihre Fähigkeiten kontinuierlich weiterzuentwickeln, um mit der ständig fortschreitenden Welt der IT Schritt zu halten.

Kai rundet seine Schilderung der essentiellen Soft-Skills mit folgenden Hinweisen ab: «Im Bereich der Awareness-Kampagnen ist die Fähigkeit, sich in die Lage eines anderen hineinzuversetzen, von entscheidender Bedeutung, um sicherzustellen, dass das Wissen nicht nur vermittelt, sondern auch tatsächlich verinnerlicht wird - Empathie wird daher eines der wirksamsten Werkzeuge im Repertoire eines effektiven Phishing-Awareness Spezialisten sein.»

Peter Kosel, Gründer, Talent Community Manager und Pionier des KNOW YOUR TALENTS-Rekrutierungsansatzes bei cyberunity fasst die Sache wie folgt zusammen:

«Bei aller Vorsicht müssen wir darauf achten, dass wir in diesem neuen Sicherheitswahn nicht paranoid werden. Wenn wir uns so stark vor allem schützen, dass es geschäftsbehindernd wird, ist auch keinem gedient. Sich von der Angst überwältigen zu lassen, würde dazu führen, dass wir alle unsere Geräte abschalten - dann wäre zwar alles sicher, aber so ziemlich jeder wäre arbeitslos. Die Kunst besteht darin, das Thema Phishing Awareness so anzugehen, dass es sowohl für Unternehmen von Vorteil ist, als auch von Kunden und Mitarbeitenden als existenzschützender und nachhaltiger Mehrwert angesehen wird - und das geht nur, wenn sich Arbeitgeber der Wichtigkeit von Beziehungspflege zu ihren Mitarbeitenden bewusst sind: Cyber Security means: KNOW YOUR PEOPLE.»