Tattoo-Marketing und Live-Chats

Einblicke in die veränderten Methoden der Cyber-Kriminalität und was sie für Unternehmen bedeuten, gab es bei einer Veranstaltung des Kompetenzzentrums Sicheres Österreich (KSÖ) mit dem Profiling-Experten Mark T. Hofmann in Wien.

Vor wenigen Jahren waren der rote Bildschirm auf einem gehackten Computer und das plötzliche Ausbleiben von Telefonanrufen nach einem Voice-over-IP-Angriff das typische Szenario, bei dem die Übertragung von Sprache über das Internet ermöglicht wurde. Das ermöglichte Angriffe wie beispielsweise Phishing. Heute hat sich das Geschäftsmodell von Hackern erweitert und verfeinert, was Unternehmen und Privatpersonen vor neue Herausforderungen stellt.

Hacker als Dienstleister. Die Taktiken von Cyber-Kriminellen haben sich professionalisiert. Neben den klassischen Methoden wie Ransomware, bei der die Daten eines Unternehmens verschlüsselt und nur gegen Lösegeldzahlung wieder freigegeben werden, drohen Angreifer jetzt, sensible Informationen auf Darknet-Marktplätzen zu veröffentlichen – oft zum Verkauf an den Meistbietenden. Die nächste Stufe ist der Einsatz von DDoS-Angriffen (Distributed Denial of Service), um Websites oder Online-Dienste lahmzulegen und Unternehmen so weiteren Schaden zuzufügen. Dabei verursachen Cyber-Kriminelle eine Vielzahl künstlicher Anfragen auf einen anvisierten Dienst im Internet. Sobald die Webserver des Opfers durch die eingehenden Anfragen überlastet sind, kommt es zu Verzögerungen und Ausfällen des betroffenen Dienstes.

Dienstleister. Neu hinzu kommt eine weitere Bedrohung, die das bisherige Verständnis von Cyber-Kriminalität grundlegend infrage stellt. Cyber-Kriminalität dreht sich nicht mehr nur um Geld oder Datendiebstahl; Hacker verstehen sich zunehmend als Dienstleister, die den emotionalen Hebel als Werkzeug einsetzen. Sie bieten Kundenservice in Form von Live-Chats oder Anrufen mit kurzen Wartezeiten an und haben ausgefeilte Marketing-Ideen: *LockBit,* eine bekannte Ransomware-Gruppe, hat im Rahmen ihrer Marketingstrategie ungewöhnliche Methoden eingesetzt, darunter das Bezahlen von Personen, die sich das *LockBit*-Logo tätowieren lassen. Diese Aktionen dienen nicht nur der Öffentlichkeitswirkung, sondern auch der Verbreitung ihrer Marke in der Untergrundszene. Berichten zufolge haben sie bis zu 1.000 US-Dollar pro Tattoo gezahlt und insgesamt 20.000 US-Dollar für solche Aktionen ausgegeben. Diese Strategie sollte *LockBit* helfen, trotz verstärkten Drucks seitens der Strafverfolgungsbehörden im Gespräch zu bleiben. „Amateure hacken Systeme, Profis hacken Menschen", lautet ein Zitat des Experten für Cyber-Sicherheit Bruce Schneier.

Die Psychologie der Cyber-Angriffe. „Cyber-Kriminalität habe selten etwas mit Ego oder einem Adrenalinschub zu tun", sagt Mark T. Hoffmann, Kriminal- und Geheimdienstanalyst. Vielmehr liege der Fokus auf den Gefühlen und Reaktionen der Opfer. Angreifer wüssten, dass Menschen oft das schwächste Glied in der Sicherheitskette darstellten. Hacker setzten auf Techniken der sozialen Manipulation (Social Engineering), um Opfer dazu zu bringen, Passwörter preiszugeben oder auf infizierte Links zu klicken. 90 Prozent der Cyber-Angriffe gingen auf menschliche Fehler zurück, Computer seien nur die Waffe.

Cyber-Kriminalität: Hacker bieten als „Dienstleister" zunehmend auch „Kundenservice" in Form von Live-Chats oder Anrufen mit kurzen Wartezeiten an

ZUR PERSON

Mark T. Hofmann ist Kriminal- und Geheimdienstanalyst und studierter Organisationspsychologe. Er hat sich auf das Verhaltens-Cyber-Profiling spezialisiert und wissenschaftliche Interviews mit Psychopathen & Hackern geführt, um die Innenperspektive zu verstehen. In den USA wurde er Teil eines offiziellen Zertifizierungsprogrammes des Justizministeriums des US-Bundesstaates Kalifornien und wurde in Profiling- und nachrichtendienstlichen Techniken ausgebildet.

Als Redner, Referent und Berater für Verhaltens-Profiling ist er international im Einsatz, primär in Europa und den Vereinigten Arabischen Emiraten. Er spricht Deutsch, Englisch, Französisch und grundlegendes Arabisch. Zu seinen Kunden zählen Global Player, Innovationstreiber, Behörden und Spitzenverhandler der Wirtschaft.

FOTOS: KATHARINA SCHIFFL, ACRONYM - STOCK.ADOBE.COM

Cyber-Kriminalität ist von männlichen Tätern dominiert – die Mehrheit der Hacker ist unter 30 Jahre alt, viele fangen bereits in der frühen Jugend, motiviert durch Spaß und Talententwicklung, an. Doch auch hier ist ein Wandel absehbar. Experten prognostizieren, dass der Frauenanteil auf der „dunklen Seite" der IT in den nächsten Jahren weiter ansteigen wird.

Neue Bedrohungen. Die Nutzung von Deepfake-Technologie nimmt rasant zu und ist dabei, die Art und Weise, wie Cyber-Kriminalität betrachtet wird, zu revolutionieren. In einem prominenten Fall in Dubai wurde die Stimme eines Bankdirektors gefälscht und ein Mitarbeiter dazu gebracht, 35 Millionen Dollar auf ein Konto zu überweisen. Für solche Täuschungen braucht es oft nur ein hochauflösendes Foto oder eine kurze Audioaufnahme.

„Das Erstellen täuschend echter Videos und Audios zur Manipulation ist keine große technische Herausforderung mehr und ermöglicht es Hackern, mit minimalem Aufwand großen Schaden anzurichten", führt Hoffmann aus und betont, dass Deepfakes in den nächsten Jahren zu einer entscheidenden Waffe im Arsenal von Cyber-Kriminellen würden. Die Herausforderung bestehe nun darin, die Öffentlichkeit für diese neuen Formen der Bedrohung zu sensibilisieren und Schutzmechanismen zu entwickeln.

Cyber-Sicherheit. Das Schlagwort lautet „Awareness" – die beste Verteidigung ist ein durchdachtes Bewusstsein für Cyber-Risiken. Neben technischen Maßnahmen wie Firewalls, Verschlüsselung und regelmäßigen Updates spielt der Faktor Mensch eine entscheidende Rolle. Schulungen, um das Bewusstsein der Mitarbeiterinnen und Mitarbeiter zu stärken, sind für Unternehmen unerlässlich. Diese „menschlichen Firewalls" können verhindern, dass Cyber-Kriminelle mit ihren emotional manipulativen Methoden Erfolg haben.

Um der Bedrohung durch solche Angriffe Herr zu werden hat das FBI die Verfolgung von Ransomware-Gruppen intensiviert. Trotzdem betonen Experten, dass die Eigenverantwortung jedes Unternehmens und jedes Einzelnen bei der Prävention eine entscheidende Rolle spielt. Vorsicht ist auch bei alltäglichen Aktionen geboten: Die Grundregeln, dass kein öffentliches WLAN für sensible Transaktionen genutzt, keine unbekannten USB-Sticks angesteckt und keine verdächtigen Anhänge geöffnet werden sollten, sind eine erste wichtige Verteidigungslinie.

Die Verantwortung für Cybersicherheit liegt nicht nur bei den Unternehmen, sondern auch bei jedem Individuum. Der Umgang mit Cyber-Kriminalität muss ebenso unterhaltsam wie informativ gestaltet sein, um das Interesse der Menschen zu wecken und damit das Verhalten nachhaltig zu verändern. Schließlich ist Cyber-Sicherheit nicht nur eine technische, sondern auch eine soziale Herausforderung.

In einer Zeit, in der Cyber-Kriminelle zunehmend raffinierter und ihre Methoden gefährlicher werden, ist der Aufbau eines ganzheitlichen, wachsamkeitsorientierten Sicherheitskonzepts wichtiger denn je. Mit der richtigen Mischung aus Technik, Schulung und präventiven Maßnahmen können Unternehmen und Einzelpersonen eine starke Verteidigung gegen die wachsende Bedrohung aus dem digitalen Raum aufbauen. *Nicole Felicitas Antal*