TECHNOLOGISCHER FORTSCHRITT & IT-FORENSIK

LEICHTES SPIEL: HACKING AS A SERVICE

Gibt es den typischen Hacker? Und wenn ja, was zeichnet ihn aus, wie und mit wem arbeitet er? Und vor allem: Sind eigentlich alle Hacker böse? Welche Spuren hinterlassen Hacker bei ihrer Tätigkeit im Netz und wie kann man diesen folgen?

Der Begriff „Hacker" ist in der Öffentlichkeit häufig negativ behaftet. Um eine Unterscheidung zwischen vermeintlich gut und vermeintlich böse herauszuarbeiten, haben sich schon vor Jahren Begriffe wie „White hat"- und „Black hat"-Hacker etabliert. Die Kenntnisse und Fähigkeiten beider Lager sind dabei oft vergleichbar – nur der Zweck, für den diese eingesetzt werden, unterscheidet sich.

LÄNGST PASSÉ: COMPUTER-NERDS IM KELLER ODER EINSAMER WOLF

Die Klischees des einsamen Wolfs oder einzelner aus Kellern operierender Computer-Nerds sind jedoch größtenteils überholt. Natürlich mag es auch diese Charaktere noch vereinzelt geben, aber Team-Play wird mittlerweile großgeschrieben und Hacker sehen sich längst als Dienstleister

Hacken, ob für die „gute" oder die „böse" Seite, braucht Spezialisten. Doch auch „gute" Vorlagen können mit geringem Aufwand für „böse" Zwecke umgemünzt werden. Oft braucht es nur jemanden, der eine mehr oder weniger ausgereifte Anwendungslösung bastelt, die dann auch oft von normalen Kriminellen als Anwender genutzt wird. Über Plattformen in schwer zugänglichen Teilen des Internets, auch unter Begriffen wie „Darkweb" bekannt, kann sich heute theoretisch jeder Otto-Normalbürger ohne großes Vorwissen diese Lösungen kaufen und sie dann anwenden („Software as a Service").

GELEGENHEIT MACHT DIEBE: ANGRIFFE NICHT IMMER ZIELGERICHTET

Dass Angriffe dabei immer zielgerichtet sind, ist ebenfalls ein Irrglaube. Ransomware-Attacken sind in den letzten Monaten stark ansteigend – allerdings in den häufigsten Fällen aufgrund von bestehenden Lücken oder Schwachstellen im System, und nicht aufgrund des bekannten Unternehmensnamens oder finanzieller Stärke. Frei nach dem Motto: „Gelegenheit macht Diebe". Fest steht: Sicherheitslücken laden Hacker ein.

LAIENFREUNDLICH: RANSOMWARE AS A SERVICE

Für Schwachstellen und Informationen, die einen Zugriff ermöglichen, gibt es ebenfalls einen florierenden Schwarzmarkt. Mit den hier erkauften Informationen und den hinzu erworbenen anwenderfreundlichen Lösungen (zum Beispiel „Ransomware as a Service") sind auch weniger qualifizierte Angreifer in der Lage, erfolgreich hohe Lösegeldsummen zu erpressen.

Ähnliches gilt für Stimmsynthese-Software (Audio-Deepfakes) und Software zur Erstellung sogenannter Video-Deepfakes. Bei Deepfakes handelt es sich meist um Bild- oder Tonmanipulation, die mit Hilfe

von lernenden KI-Modellen vorgenommen werden. Täuschend echte Stimmmanipulationen können mittels Video-Tutorials auf öffentlichen Videoplattformen von jedermann erstellt werden. Der Aufwand dafür ist nicht besonders hoch. Diese Stimmprofile können dann beispielsweise verwendet werden, um „Fake-President"-Angriffe zu initiieren oder gezielte Diffamierungskampagnen zu starten.

HEUTE SCHON TECHNISCH MÖGLICH: ECHTZEIT-UNTERHALTUNGEN IN DEEPFAKES

Für den Erfolg eines CEO Fraud ist oft das „Social Engineering" entscheidend. Für diese Manipulation der designierten Opfer ist eine Konversation in Echtzeit notwendig, die Wertschätzung ausdrückt und Bedenken zerstreut, Druck aufbaut oder Fragen beantwortet. Solche Konversationen in Echtzeit sind heute technisch längst möglich – sowohl als Audio- als auch als Video-Deepfake.

Das bedeutet: Auch manipulierte Video-Calls, in denen ein gefälschter CEO mit dem richtigen Aussehen und der richtigen Stimme Anweisungen für Überweisungen gibt, sind möglich. Das schafft ein maximales Vertrauen in die Echtheit des Auftrags, und die Ausführenden dürften in vielen Fällen gar keinen Verdacht schöpfen. Das hebt das Social Engineering – und die Möglichkeiten, die sich Betrügern damit bieten – auf eine ganz neue Ebene.

WAS TUN NACH EINEM ANGRIFF?

Die Gefahr, selbst zum Opfer von Cyberkriminellen zu werden, steigt mit der rasanten Entwicklung der Technologie. Doch was tun, wenn ein Angriff erfolgt ist? Dann müssen Unternehmen vor allem schnell und bewusst handeln. Warum bewusst? Weil zu schnell getroffene Entscheidungen weitreichende Folgen haben können. Unternehmen müssen unbedingt rechtliche Risiken im Auge behalten, unter anderem im Bereich Datenschutz, Arbeitsrecht oder auch im Hinblick auf vertragliche Verpflichtungen. Die zu erwartenden Sanktionen müssen unbedingt in die Überlegungen und Kommunikation einbezogen werden. Dies ist eine Aufgabe, die unternehmensintern oft nur dann abgebildet werden kann, wenn Szenarien bereits zuvor geplant und geprobt wurden. Ansonsten sind Unternehmen gut beraten, auf externe Dienstleister zurückzu-greifen, die in dieser oft emotionalen und hektischen Situation mit einem neutralen Blick die Sachlage einschätzen. Schnell ja – aber ein unüberlegter Schnellschuss kann nach hinten losgehen.

72 STUNDEN: DIE UHR TICKT!

Meist spielen bei einem Cyberangriff die ersten 72 Stunden eine absolut kritische Rolle. IT-Forensiker haben kein großes Zeitfenster, um Spuren im Netz nachzugehen und eventuell noch zu retten, was zu retten ist. Die NASA fährt nach kritischen Ereignissen beispielsweise die Schotten runter: „Lock the doors!" Nach diesem Kommando sichern alle am Projekt Beteiligten ihre Daten und schreiben in Gedächtnisprotokollen die letzten Vorgänge und Minuten vor dem Ereignis auf.

Dieses Vorgehen wäre für einen Forensiker nach einem Sicherheitsvorfall jeglicher Art optimal. Gleichzeitig ist das in einem arbeitenden Unternehmen meist illusorisch. Das liegt schon allein daran, dass Sicherheitsvorfälle oft erst mit Verzögerungen festgestellt werden. Es ist daher wichtig, die Situation so weit wie möglich einzufrieren, ohne jedoch den Betriebsablauf weiter unnötig zu schwächen.

Sobald möglichst viele Informationen idealerweise beweissicher festgehalten wurden, muss das Unternehmen diese Informationen in Ruhe sichten und weitere Schritte einleiten. Diese Schritte können aus zivilrechtlichen und strafrechtlichen Maßnahmen bestehen. Je nach Tathergang ist es im Internet jedoch sehr schwer, die Täter hinter den Zugriffen technisch auszumachen. Das Internet ist zwar nicht anonym und technische Spuren lassen sich nicht bis in das letzte Detail verwischen, aber eine internationale Strafverfolgung stößt immer wieder an ihre Grenzen. Hinzu kommt, dass Tätergruppen teilweise auch von ihren Heimatstaaten geschützt oder wissentlich nur schwach verfolgt werden.

Dennoch hilft eine schnelle Reaktion häufig, zumindest einen Teil der erbeuteten Gelder oder Daten wieder zurückzuholen. Eine erfolgreiche Zusammenarbeit mit Banken ist dabei essenziell, um Konten rasch einzufrieren – bevor Geld verschoben und verloren ist.

Autor dieses Beitrags ist Dirk Koch, Rechtsanwalt & Data Protection Risk Manager.