Mark T. Hofmann, Kriminal- & Geheimdienstanalyst, zum Thema Cyberkriminalität im Medizinsektor

Prof. Martin Heubner im Gespräch mit Mark T. Hofmann

Zur Person

Mark T. Hofmann ist Kriminal- & Geheimdienstanalyst und Organisationspsychologe (M. A.). Er hat sich auf das Verhaltens- & Cyber-Profiling spezialisiert und anonyme Interviews mit Hackern geführt, um die Innenperspektive zu verstehen. Als Referent und Keynote Speaker begeistert er Menschen auf der ganzen Welt für das Thema Cybersecurity und zeigt, wie wir zu einer „menschlichen Firewall" werden können. Er ist bekannt durch internationale TV-Formate (CNN, ARD, CBS, Forbes, 60 Minutes Australia u. v. m). Zu seinen Kunden zählen Unternehmen jeder Größe, Banken, Krankenhäuser, Behörden und Spezialeinheiten der Polizei.

Haben Sie Interesse, mehr zu erfahren? Mit untenstehendem QR-Code gelangen Sie zum Vortrag *Profiling Hackers: Die Psychologie der Cyberkriminalität* von Mark T. Hofmann (www.mark-thorben-hofmann.de/cybercrime).

Prof. Martin Heubner: *Herr Hofmann, Sie sind Kriminalanalyst und Organisationspsychologe und beschäftigen sich schwerpunktmässig mit Cyberkriminalität. Viele Firmen sind bereits durch Hackerangriffe geschädigt worden, einige haben grosse Geldsummen gezahlt, um nach einem Angriff ihre Daten wiederzubekommen. Sind Arztpraxen oder Spitäler eigentlich auch im Fokus von Kriminellen? Stellen nicht Wirtschaftsunternehmen wie Banken oder Logistikunternehmen viel lukrativere Opfer dar?*

Mark T. Hoffmann: „Ransomware" ist eine der größten Gefahren für Unternehmen und auch KRITIS (= kritische Infrastruktur, z. B. die Bereiche Energie, Wasser, Transport, Gesundheit, Telekommunikation oder Banken). Daten werden verschlüsselt, nichts geht mehr, alles steht still. Ein Lösegeld wird verlangt, sonst werden die Daten gelöscht oder – schlimmer sogar – Patientendaten im Darknet veröffentlicht. In der Wirtschaft kostet so ein Stillstand Geld, im Krankenhaus geht es schnell um Menschenleben. Die Notlage und die Dringlichkeit sind noch höher und somit auch die Zahlungsbereitschaft.

So schwer es manchmal fällt, bedeutet „Profiling", die Tat aus der Perspektive der Täter zu sehen. Aus Tätersicht gibt es drei wesentliche Entscheidungskriterien:

– Wie viel Geld ist zu holen (Höhe des möglichen Lösegeldes)?
– Wie groß ist die Wahrscheinlichkeit, dass gezahlt wird (Zahlungsbereitschaft)?
– Wie einfach oder aufwändig ist der Angriff (Weg des geringsten Widerstands)?

Manchmal spielt auch die Entdeckungswahrscheinlichkeit eine Rolle, aber leider selten, da diese ohnehin gering ist. Manche Gruppen haben auch „moralische Prinzipien" – bewusst in Anführungsstrichen – und greifen grundsätzlich keine Krankenhäuser an. Um die Frage klar zu beantworten: Natürlich ist bei klassischen Unternehmen mehr zu holen, bei Krankenhäusern ist durch die akute Notlage aber oft die Zahlungsbereitschaft höher und sie sind schlechter geschützt.

Können Sie über die letzten Jahre eine Entwicklung beobachten, was die Cyberkriminalität im Gesundheitssektor angeht?

Absolut, die Bedrohungslage im Gesundheitssektor (auch in der Schweiz) hat sich verschärft. Große Angriffe auf Kliniken in Düsseldorf oder Barcelona sind da eher die Spitze des Eisbergs. Dass BKA hat bereits 2020 einen Anstieg von Ransomware verzeichnet und stellt fest: „Attacken auf KRITIS, z. B. Krankenhäuser und Wasserwerke, zeigen, dass erfolgreiche Ransomware-Angriffe drastische Folgen für die Zivilbevölkerung nach sich ziehen und elementare Services des öffentlichen Geschehens sabotieren können." (BKA Deutschland, Bundeslagebild 2020)

Cybersicherheit und Digitalisierung müssen Hand in Hand gehen. Je vernetzter und automatisierter wir arbeiten, desto angreifbarer werden wir.

Wie laufen Cyberattacken üblicherweise *ab?*

Das am meisten unterschätzte Sicherheitsrisiko ist der Mensch. Mehr als 90 % der Cyberangriffe gehen auf menschliche Fehler zurück. Damit ist Cybercrime kein rein technisches, sondern auch ein psychologisches Phänomen. Es braucht also technische Sicherheit, aber auch Mitarbeiter und Mitarbeiterinnen müssen sensibilisiert werden, denn

es sind Menschen …,
… die Anhänge mit Schadsoftware öffnen oder auf Links in Phishing-Mails klicken;
… die am Telefon das Passwort verraten, wenn jemand behauptet, „vom IT-Support" zu sein;
… die USB-Sticks aus Neugierde anstecken, die sie auf dem Parkplatz gefunden haben;
… die sich in fremde WIFI-Netzwerke einloggen;
… die ihre Laptops unentsperrt stehen lassen, um eine Zigarette zu rauchen;
… die auf gefälschte Anrufe oder E-Mails hereinfallen, in denen sich Betrüger als Vorgesetzte ausgeben;
… die in der Bahn oder am Flughafen zu sensiblen Themen laut telefonieren;
… die ihre Zugangsdaten zum System auf einem Post-It-Notizzettel notieren und neben den PC kleben;
… die Dokumente im Kopierer oder Drucker auf dem Flur liegen lassen etc.

In meinen Vorträgen probiere ich immer zu zeigen, dass wir eine Kombination aus einer technischen und einer „menschlichen Firewall" brauchen.

Viele fragen sich ja, was für Menschen hinter den Attacken stecken. Unterscheiden diese sich von „gewöhnlichen" Kriminellen und Betrügern?

Hacker werden medial gerne bildlich dargestellt als 15-jährige Teenager in schwarzen Kapuzenpullovern. Natürlich gibt es auch Einzeltäter, die größere Gefahr

geht aber von Gruppen aus. Polizei und Nachrichtendienste sprechen gerne von „Crime-as-a-Service“, da diese Gruppen mittlerweile nicht nur wie Unternehmen agieren, sondern sogar professioneller als Unternehmen. Es ist mittlerweile ein richtiger Markt mit Support, Qualitätsmanagement und Provisionsmodellen. Da Spitäler zur kritischen Infrastruktur zählen, ist leider auch (politisch motivierter) Cyber-Terrorismus eine mögliche Gefahr in Zeiten geopolitischer Spannungen.

So etwas wie ein „Standardprofil“ gibt es nicht, es lässt sich aber schon sagen, dass es meist junge Männer sind, überdurchschnittlich intelligent, überdurchschnittlich gut gebildet, kein niedriger sozioökonomischer Status, und „thrill seeking“ (der „Kick“) ist oft Teil der Motivation. Zumindest bei Tätern, die längst genug Reichtum angehäuft haben und dennoch weiter, weiter und weiter machen, ist das Motiv nicht Geld, sondern Gier.

Die Digitalisierung im medizinischen Sektor nimmt nach relativ langer Verzögerung aktuell recht an Fahrt auf. Sehen Sie zusätzliche Risiken durch die vermehrte Anwendung von Apps für Mobilgeräte, Online-Anmeldungen oder Ähnliches auf uns zukommen?

Ja, aber die Lösung besteht auch nicht darin, zurück zu Papier und Bleistift zu gehen. Wer jetzt nicht digitalisiert, wird 2030 wahrscheinlich ohnehin keine Rolle mehr spielen. Die Technik wird weiter voranschreiten, aber es ist wichtig, auch die Gefahren im Blick zu haben und in Cybersicherheit zu investieren. Auch Autos führen zu mehr Verkehrsunfällen, aber die Forderung, zur Kutsche zurückzukehren, erscheint mir ähnlich realitätsfern wie eine De-Digitalisierung.

Gibt es ein paar Faustregeln, die Sie als Schutz vor solchen Angriffen empfehlen können?

Natürlich: Lange, komplexe und unterschiedliche Passwörter verwenden. Auch privat ein Virenschutzprogramm. Vorsicht bei externen W-LANS, USB-Sticks oder Anhängen. Unbedingt zurückrufen, sollte Ihnen ein Anruf oder eine E-Mail seltsam vorkommen.

Von Phishing per Mail bis Identitätsdiebstahl oder CEO-Fraud: Häufig kommen drei Elemente zusammen: Starke Emotion wird ausgelöst (Notfall), Zeitdruck wird aufgebaut (Sie sollen SOFORT handeln) und Sie werden um etwas Ungewöhnliches gebeten (z. B. Blitzüberweisung oder Passwort verraten). Wenn diese drei Dinge zusammenkommen, sollte man zumindest einen Plausibilitäts-Check machen: Stimmt die E-Mail-Adresse? Ist die E-Mail fehlerfrei? Ist eine persönliche Anrede enthalten? (Keine Bank schreibt Ihre Kunden heute noch mit „Lieber Kunde“ an.) Würde mein/e Chef/Chefin mich wirklich Samstag um 21:00 Uhr um eine Blitzüberweisung bitten? Würde der Zoll mir tatsächlich eine Mail schreiben mit einem Anhang? Wieso bekomme ich eine Paketbenachrichtigung, ohne etwas bestellt zu haben?

Das Stichwort ist „Cybersecurity Awareness“: Wer die Gefahren kennt, nimmt ihnen den Wind aus den Segeln.

Vielen Dank für das informative Interview!