Unfreiwillig gläsern – oder wenn ein Staatstrojaner auf die Berufswelt trifft

INTERVIEW mit Ass. jur. Paul H. Malberg

Der Detektiv und Jurist Paul H. Malberg erzählt, wie sein Unternehmen die mächtige Spionagesoftware Pegasus auf dem Handy eines ehemaligen Bankmanagers entdeckte, welche Herausforderungen sein Team dabei meistern musste und warum der Fall weitreichende Konsequenzen haben könnte.

Ass. jur. Paul H. Malberg
ist Geschäftsführer der Detektei PROOF-MANAGEMENT GmbH in Hamburg, Düsseldorf, Frankfurt/M. und Köln.

ZAU: Herr Malberg, in unserem letzten Interview haben Sie sich noch als Detektiv der Wirtschaft vorgestellt. Dabei ging es im Wesentlichen um die Aufklärung von Straftaten insbesondere durch Mitarbeiter. Betreiben Sie jetzt auch Spionageabwehr gegen ausländische Geheimdienste?

Malberg: In dem von Ihnen angesprochenen Fall scheint das tatsächlich so zu sein. Aber fangen wir am Anfang an:
Unser Kunde, eine ehemalige Führungskraft aus dem Bankensektor, kontaktierte uns im Dezember letzten Jahres, nachdem er verschiedene Anomalien – so u.a. veränderte Chatverläufe – auf seinem iPhone bemerkt hatte. Er vermutete, dass ohne sein Wissen eine Schadsoftware installiert worden sein könnte, und bat unsere Detektei um eine IT-forensische Untersuchung des Geräts.

ZAU: Was waren Ihre ersten Gedanken und Schritte, als Sie den Fall übernommen haben?

Malberg: Zunächst muss ich betonen, dass Handys bzw. mobile Endgeräte tatsächlich des Öfteren mit sog. Malware infiziert werden. Das geschieht etwa durch breit angelegte Angriffe auf einen großen und unbestimmten Personenkreis.
Manchmal werden bestimmte Personen aber auch gezielt ins Visier genommen. Überwiegend gelingen solche Angriffe in der Masse bei Geräten mit einem Android-System, hingegen seltener bei Geräten der Marke Apple mit iOS-Systemen. Dass es sich im Fall unseres Kunden aber um eine Malware handeln könnte, die von staatlichen Einrichtungen verwendet wird, hatte ich aufgrund der Schilderungen unseres Kunden zunächst nicht angenommen.
Wir führten also im ersten Schritt routinemäßig eine forensische Analyse der Datenoberfläche durch. Hier konnte jedoch kein Hinweis auf eine Malware gefunden werden, sodass der Befund negativ war.

ZAU: Wie konnten Sie sich dann die Anomalien, von denen Sie gesprochen haben, erklären?

Malberg: Bis hierhin gar nicht. Wir hatten keine Erklärung, waren aber wegen der vom Kunden angesprochenen Auffälligkeiten auf manipulierte Daten überzeugt, dass es hierfür eine Erklärung geben müsse.
Wir schlugen dem Kunden schließlich vor, mittels eines sog. „Jailbreaks" (bei Android „root" genannt) in das tiefere und herstellerseitig besonders geschützte System der Hardware vorzudringen. Dazu gehört es, die „Tür" zum Betriebssystem des betroffenen Geräts „aufzubrechen", um auf tiefere Ebenen des Systems zugreifen und diese forensisch prüfen zu können. Diese Maßnahme ist dann notwendig, wenn besonders perfide Trojaner aufgespürt werden sollen, die bereits einen erheblichen Grad an Gefährlichkeit und Professionalität aufweisen.

ZAU: Und das führte dann zum Erfolg?

Malberg: So einfach war das leider nicht. Denn der später gefundene High-End-Trojaner Pegasus ist wirklich ein Profi darin, seine Spuren zu verwischen und überdies zu verhindern, dass er lokalisiert wird. Selbst nach zig Versuchen eines Jailbreaks war es zunächst nicht möglich, einen vollständigen Zugriff auf das gesamte Handy zu erhalten.
Unser Forensiker formulierte zur Veranschaulichung folgenden zutreffenden Vergleich: Stellen Sie sich vor, Sie sind professioneller Autodieb und auf Oberklasse-Pkw spezialisiert. Dann kennen Sie sich mit jeder Luxusmarke und deren Autos aus. Sie wissen in- und auswendig, wie Technik, Sicherheitssysteme wie Wegfahrsperren und Autoschlösser funktionieren. Und falls es sich bei dem begehrten Objekt nicht gerade um ein brandneues Fahrzeugmodell handelt, dann sind Sie als passionierter Autodieb vorbereitet und knacken das Auto in einer zuvor gut geschätzten Zeit.
Das Beispiel lässt sich gut auf das konkrete iPhone-Modell, um das es hier ging, übertragen. Normalerweise ist bei diesem Modell ein Jailbreak reine Routine. Doch es hat nicht funktioniert. Erst nach vielen Stunden und intensiver Zusammenarbeit mit internationalen Experten erlangten wir den vollständigen Zugang zum Handy.

ZAU: Wie haben Sie schließlich die Anwesenheit von Pegasus bestätigt und wie war Ihre Reaktion?

Malberg: Nachdem wir die Schutzmechanismen erfolgreich ausgehebelt hatten, führten wir eine 20-stündige Softwareanalyse durch, die über 13.000 Dateien überprüfte. Diese Analyse identifizierte schließlich zehn infizierte Dateien mit dem klaren Befund „NSO-Pegasus".
Ich kann mich gut daran erinnern, wie mich mein Mitarbeiter an einem Samstag aufgeregt anrief und meinte, dass unser Kunde den „Jackpot" gewonnen habe, allerdings den negativen. Er konnte selbst kaum fassen, was ihm das System ausgeworfen hatte. Auf meine Frage, ob das Ergebnis zu 100% sicher sei, meinte er nur: *„Herr Malberg, ich habe so etwas auch noch nie gesehen."* Und europaweit wurde der Trojaner Pegasus, soweit uns das bekannt ist, erst drei bis vier Mal gefunden.
Es war ein intensiver, mühsamer und zeitaufwendiger Prozess, der bis dato beispiellos war. Aber der Befund war eindeutig.

ZAU: Was müssen sich die Leser denn unter einem Trojaner mit dem Namen Pegasus vorstellen?

Malberg: Pegasus ist ein in der Branche bekannter Trojaner und eine Art von Spyware, die von der israelischen Firma NSO Group entwickelt und meines Wissens erstmals 2016 von

Foto: istockphoto/cosmin4000

„Auch Führungskräfte, Manager und theoretisch sogar reguläre Mitarbeiter mit Spezialwissen können potenzielle Ziele für staatliche Akteure, Wettbewerber oder andere Interessengruppen sein."

einem Sicherheitsunternehmen entdeckt wurde. Ursprünglich wurde Pegasus als ein Werkzeug für Regierungen und Behörden zur Bekämpfung von Terrorismus und schweren Verbrechen konzipiert und verkauft. Die Software ermöglicht es, z.B. Mobiltelefone ohne das Wissen der Benutzer zu überwachen und zu infiltrieren.

Der Trojaner Pegasus ist besonders umstritten, weil er in der Lage ist, sog. „Zero-Click"-Angriffe durchzuführen. Das bedeutet, dass das Zielgerät theoretisch ohne jegliche Interaktion des Benutzers infiziert werden kann. Diese Angriffe nutzen Schwachstellen in mobilen Betriebssystemen aus, um die Software heimlich zu installieren. Einmal installiert, kann Pegasus nahezu alle Daten auf einem Smartphone überwachen und stehlen, einschließlich Nachrichten, Anrufe, E-Mails, Fotos sowie Videos, und es kann sogar auf Mikrofon und Kamera des Geräts zugreifen, um Live-Überwachungen durchzuführen.

Pegasus ist global sehr umstritten, da er Medienberichten nach häufig missbraucht wurde, um Journalisten, Menschenrechtsaktivisten, politische Führer und Persönlichkeiten des öffentlichen Lebens auszuspionieren. Das hat zu erheblichen Bedenken hinsichtlich der Menschenrechte und der Privatsphäre geführt. Enthüllungen durch verschiedene Medien und Menschenrechtsorganisationen wie Amnesty International schätzen, dass Pegasus weltweit von mindestens 40 Ländern eingesetzt wurde, oft in Situationen, die über die behaupteten Zwecke der Bekämpfung von Terrorismus und Kriminalität hinausgehen. Diese Enthüllungen haben zu Forderungen nach strengeren Kontrollen und einem Moratorium für den Einsatz solcher Überwachungstechnologien geführt.

Die Entdeckung, dass Pegasus zur Überwachung hochkarätiger Persönlichkeiten und sogar zur Verfolgung von Familienmitgliedern des ermordeten Journalisten *Jamal Khashoggi* verwendet wurde, hat die Kontroversen weiter verschärft. Trotz der Behauptungen von NSO Group, dass sie nur an legitime staatliche Stellen verkauft und die Menschenrechtslage ihrer Kunden überprüft hätten, scheint es so, dass die Software oft für illegale Überwachung und Missbrauch verwendet wurde.

ZAU: Wie ging es dann weiter und wie haben die Behörden auf Ihre Entdeckungen reagiert?

Malberg: Unserem Kunden war es immens wichtig, dass der Befund weiter untersucht wird. Allerdings lag es verständlicherweise nicht mehr in seinem Interesse, hierfür die Kosten selbst tragen zu müssen. Er wendete sich also mit unserem Bericht an die zuständigen Ermittlungsbehörden, deren Reaktion nach unserer Einschätzung eher verhalten war, vielleicht sogar als schleppend bezeichnet werden kann.

Trotz der für uns eindeutigen Befunde und eine weitere Bestätigung durch ein Labor des Softwareherstellers fühlten sich die Ermittler scheinbar nicht sonderlich alarmiert. Es dauerte recht lange, bis sie sich das betroffene Gerät überhaupt anschauen wollten, was für unseren Kunden, aber auch für uns überaus frustrierend war.

Möglicherweise stieg das Interesse der Behörden auch erst dann, als sich unser Kunde mit seinen Erlebnissen an Journalisten vom Handelsblatt wandte, die wiederum eine Presseanfrage bei den bis dato involvierten Behörden stellten und anschließend einen Artikel zu dem Thema veröffentlichten. Erst im Anschluss wurde unser Forensiker gebeten, das Handy an die zuständige Polizeibehörde zu übergeben. Aktuell laufen die Ermittlungen noch.

ZAU: Was sind Ihrer Meinung nach die weitreichenden Konsequenzen dieses Falls insb. für die Wirtschaft?

Malberg: Der Fall zeigt deutlich, dass selbst Führungskräfte in Unternehmen nicht vor Cyberüberwachung sicher sind und mit einem unentdeckten Angriff rechnen müssen. Pegasus wurde ursprünglich entwickelt, um Kriminelle und Terroristen zu überwachen, aber die Entdeckung dieser Spyware auf dem Gerät einer wirtschaftlich aktiven Person unterstreicht, dass auch Führungskräfte, Manager und theoretisch sogar reguläre Mitarbeiter mit Spezialwissen potenzielle Ziele sind. Ihre Positionen können sie zu interessanten Zielen für staatliche Akteure, Wettbewerber oder andere Interessengruppen machen, die sensiblen Zugang zu Geschäftsgeheimnissen, strategischen Plänen oder persönlichen Informationen suchen.
Die Möglichkeit, dass Pegasus für Wirtschaftsspionage verwendet wird, stellt eine große Bedrohung dar. Angreifer könnten über diese Software vertrauliche Informationen wie Geschäftsstrategien, Kundenlisten, Preisgestaltungen, Finanzdaten und mehr abgreifen. Dies kann nicht nur zu einem erheblichen finanziellen Verlust führen, sondern auch das Vertrauen der Kunden und Partner in das Unternehmen untergraben. Die Tatsache, dass hochentwickelte Überwachungstools wie Pegasus in den falschen Händen verwendet werden können, unterstreicht die Notwendigkeit für Unternehmen, ihre Sicherheitspraktiken zu überdenken und zu verstärken.

ZAU: Was raten Sie Menschen, die ähnliche Verdachtsmomente haben?

Malberg: Ich rate dringend, professionelle Hilfe in Anspruch zu nehmen. Selbst die besten Antivirenprogramme sind oft nicht in der Lage, hochentwickelte Spionagesoftware zu erkennen. Eine gründliche und regelmäßige forensische Untersuchung gibt Aufschluss über die tatsächliche Bedrohung. Und es ist wichtig, jede verdächtige Aktivität ernst zu nehmen und rechtzeitig zu handeln.

ZAU: Können Sie unseren Lesern abschließend noch etwas zum Nutzen von professioneller IT-Forensik mit auf den Weg geben?

Malberg: Wenn Ihre Leser den Verdacht haben, dass ein Mitarbeiter die betriebliche IT missbräuchlich genutzt hat, kann es – wie ein weiterer Fall bei uns gezeigt hat – verheerende Folgen haben, etwaige vermeintliche Beweise für ein Fehlverhalten ohne die notwendige Fachexpertise eigenständig zu sichern. Einer unserer Kunden hatte genau das getan und aufgrund der eigenen „Erkenntnisse" einen Rechtsstreit gegen einen Mitarbeiter geführt. Da die Geschäftsführung dann aber immer mehr das Gefühl bekam, sich mit der internen Sachverhaltsklärung durch die IT-Abteilung auf Glatteis zu bewegen, bat sie uns, die Ergebnisse und Dokumentation, auf die sich die Klage stützte, IT-forensisch zu verifizieren.
Und siehe da: Unser Forensiker fand leider diverse Fehler bei der selbst erstellten Dokumentation, vermutlich verursacht durch mangelhaftes Wissen der IT-Verantwortlichen, die im Bereich Forensik nicht ausreichend geschult waren. Nach unserer Untersuchung brach also die selbst initiierte Klage gegen den Mitarbeiter wie ein Kartenhaus in sich zusammen. Aber Sie wissen ja: Besser ein Ende mit Schrecken als ein Schrecken ohne Ende.

ZAU: Lieber Herr Malberg, ich bedanke mich für das Gespräch!
Das Interview führte Silvio Fricke, BVAU e.V.

Foto: istockphoto/ugde