»Unternehmen müssen die Initiative ergreifen und proaktiv handeln«

Wer bei der eigenen Cyber Security nur darauf wartet, angegriffen zu werden, verschenkt wertvolle Zeit und Erfahrungen. Patrick Ungeheuer, Director of Offensive Security der Mantodea Security GmbH, plädiert deshalb für offensive, proaktive Maßnahmen, um Angreifer so früh und allwissend wie möglich abzuwehren: »Die Kombination von fortschrittlicher Technologie und menschlicher Expertise ermöglicht es uns, ein wirklich umfassendes Bild der Sicherheitslage eines Unternehmens zu erhalten und entsprechend zu handeln.«

Interview Rüdiger Schmidt-Sodingen

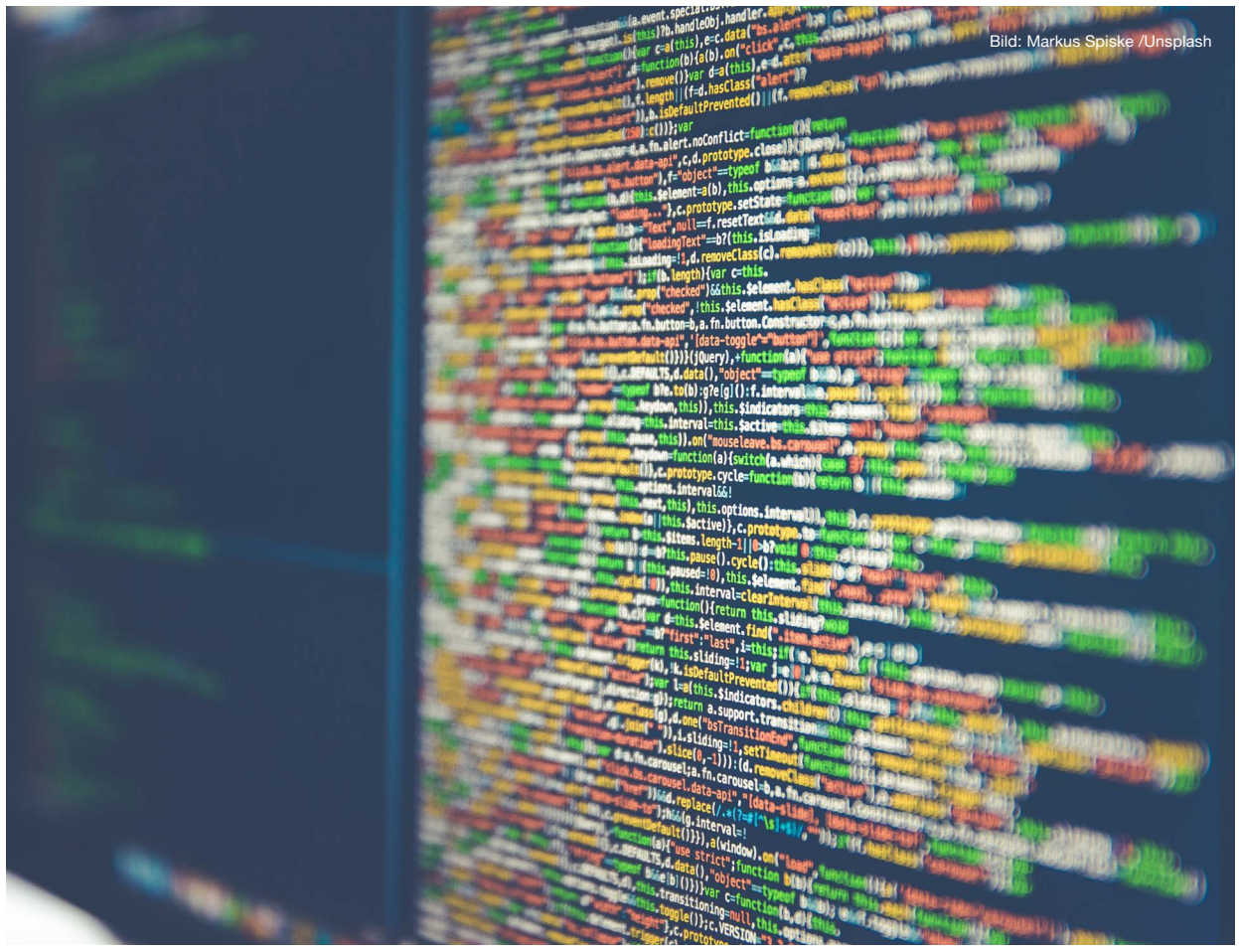
Bild: Markus Spiske /Unsplash

Herr Ungeheuer, weshalb sollten Unternehmen bei ihrer Cyber Security endlich in den »Offensive«-Modus schalten?
Stellen Sie sich vor, Sie sind Kapitän eines modernen Schiffes in stürmischen Gewässern. Würden Sie warten, bis das Wasser in den Schiffsrumpf eindringt, bevor Sie überhaupt anfangen, nach Lecks zu suchen? Natürlich nicht. Ein proaktiver Kapitän plant voraus, steuert strategisch und hat stets ein Auge auf den Horizont, um mögliche Gefahren zu erkennen und ihnen zuvorzukommen. Genau das bedeutet »Offensive« in der Cyber Security: Es geht darum, den Kurs zu bestimmen, statt von den Wellen bestimmt zu werden. In der digitalen Ära ist es nicht mehr genug, einfach zu reagieren. Unternehmen müssen die Initiative ergreifen, den Horizont scannen und proaktiv handeln. Das sollte der Leitstern für jedes fortschrittliche Unternehmen sein.

Inwiefern ist ein simulierter Angriff, das sogenannte Red Teaming, einem Penetrationstest überlegen?
Sicherheitsanalysen, oft dominiert von automatisierten Tests, liefern zweifellos einen grundlegenden Einblick, erreichen jedoch nicht die Tiefe und Breite, die manuelle Untersuchungen bieten. Penetrationstests fokussieren durch manuelle Überprüfungen spezifische Systembereiche und bringen gezielt Schwachstellen zum Vorschein. Red Teaming jedoch greift noch tiefer, indem es den gesamten Unternehmensbereich ins Visier nimmt und einen rigorosen Realitätscheck über alle Sicherheitsebenen liefert.

Die bittere Wahrheit, der sich viele Unternehmen stellen müssen, ist, dass ihre bisherigen Sicherheitsanalysen manchmal eklatante Sicherheitslücken übersehen. Bei Mantodea Security haben wir es oft erlebt: Unternehmen, die jahrelang in Sicherheitsmaßnahmen investiert haben, nur um durch unsere intensiven Penetrationstests und Red Team-Überprüfungen herauszufinden, dass ihre Systeme anfälliger waren, als sie es sich jemals hätten vorstellen können. Dies ist ein eindringlicher Weckruf zur Notwendigkeit, tiefgehende, manuelle Überprüfungen als integralen Bestandteil des Sicherheitsansatzes zu betrachten.

Nutzt »Offensive Security« Künstliche Intelligenz? Und wie kann man sich das vorstellen?
Künstliche Intelligenz ist in der Offensive Security zweifelsohne ein wertvolles Hilfsmittel. Sie agiert wie ein ständig wachsamer Wächter, der in der Lage ist, eine überwältigende Menge an Daten in Rekordzeit zu analysieren. Dabei erkennt sie Muster und bietet Prognosen, die für den menschlichen Analysten möglicherweise nicht sofort sichtbar sind. Aber es ist wichtig, sich klarzumachen: KI ist kein Allheilmittel. Der Begriff »KI« ist in letzter Zeit zu einem Buzzword geworden, aber in Wahrheit kann sie manuelle Überprüfungen durch erfahrene Analysten nicht vollständig ersetzen. Diese Experten bringen einen unschätzbaren Kontext, Intuition und Erfahrung mit, die eine Maschine nicht replizieren kann.


Patrick Ungeheuer, Director of Offensive Security der Mantodea Security GmbH

Gleichzeitig können simulierte Angriffe sehr gut auch »menschliche Schwächen« aufdecken?
Absolut, und hier sehen Sie das Zusammenspiel von Mensch und Technologie. Während KI bei der Identifizierung von Mustern in Daten hilft, sind es die menschlichen Experten, die solche simulierten Angriffe durchführen und interpretieren. Sie identifizieren Schwachstellen im menschlichen Verhalten und in unseren Prozessen. Die Kombination von fortschrittlicher Technologie und menschlicher Expertise ermöglicht es uns, ein wirklich umfassendes Bild der Sicherheitslage eines Unternehmens zu erhalten und entsprechend zu handeln.

Eignen sich offensive Methoden auch für defensive Maßnahmen oder Reaktionen?
Denken Sie an das Boxtraining. Ein Boxer, der das Blue Team repräsentiert, trainiert regelmäßig, indem er gegen einen Sandsack schlägt. Er festigt seine Schlagtechniken, verbessert seine Ausdauer und lernt, kontrolliert und präzise zuzuschlagen. Doch trotz dieser intensiven Trainingseinheiten fehlt ihm die Erfahrung eines unvorhersehbaren Gegners.

Hier kommt der Sparringspartner ins Spiel, der das Red Team repräsentiert. Anders als der Sandsack ist der Sparringspartner beweglich, reaktiv und kann selbst offensiv werden. Er bringt den Boxer in Situationen, die er mit dem Sandsack allein nie erleben würde und fördert so seine Reaktion und Anpassungsfähigkeit.

Die Zusammenarbeit von Boxer und Sparringspartner, die hier als »Purple Team« dargestellt wird, stellt sicher, dass der Boxer sich ständig weiterentwickelt. Er ist somit bestens vorbereitet, um im realen Kampf - oder in unserem Kontext, in der echten Cyber-Umgebung - bestehen zu können.

Woran liegt es, dass Firmen, die nach ISO 27001 zertifiziert sind, schon beim ersten richtigen »Offensive«-Test in kurzer Zeit zerlegt werden und nichts davon merken?
Die Zertifizierung nach ISO 27001 ist ein bedeutsamer Meilenstein für Unternehmen, jedoch darf man sie nicht als alleinigen Maßstab für durchgängige Sicherheit betrachten. Es beunruhigt, wie viele Unternehmen die Einhaltung dieses Standards als abgeschlossenes Projekt betrachten und dann in eine Art Selbstzufriedenheit verfallen, bis der nächste Audit ansteht. In einer Welt, in der sich Cyberbedrohungen ständig weiterentwickeln, können Unternehmen es sich nicht leisten, sich ausschließlich auf einen festgelegten Standard zu verlassen und darauf zu warten, dass wieder geprüft wird. Ein Zertifikat mag ein gewisses Maß an Sicherheit suggerieren, aber es ist nur der Anfang. Aktive und regelmäßige Anpassungen an die aktuellen Sicherheitsanforderungen sind unerlässlich.

Welchen Stellenwert haben Angriffssimulationen mittlerweile in Deutschland, verglichen mit anderen europäischen Ländern?
Ungeheuer: Hier müssen wir ehrlich sein. Deutschland hinkt im Vergleich zu einigen europäischen Nachbarn hinterher, vor allem aufgrund des übermäßigen Bürokratismus und alter Firmenstrukturen. Die Cyber-Security-Kultur in Deutschland ist leider immer noch nicht dort, wo sie sein sollte. Aber wir sind hier, um das zu ändern, um Deutschland auf die Überholspur zu bringen und die Art und Weise, wie wir über Sicherheit denken, neu zu definieren.

Genius Tip

»KI ist in letzter Zeit zu einem Buzzword geworden, aber in Wahrheit kann sie manuelle Überprüfungen durch erfahrene Analysten nicht vollständig ersetzen. Diese Experten bringen einen unschätzbaren Kontext, Intuition und Erfahrung mit, die eine Maschine nicht replizieren kann.«