

Wenn eine Zeile teure Folgen hat

Hacker nutzen oft Sicherheitslücken – Cirosec hat sich auf die Bekämpfung spezialisiert

Hacker arbeiten heutzutage auch mit KI, um Schwachstellen in Software und Firmennetzen zu finden. Foto: dpa

Von Heiko Fritze

HEILBRONN Stefan Strobel ist im Prinzip der Chef von professionellen Hackern: Etwa zwei Drittel seiner Mitarbeiter versuchen tagtäglich, in die IT-Systeme von Unternehmen oder Behörden einzudringen. Allerdings nicht, um Schaden anzurichten, Daten abzugreifen oder die Anlagen zu verschlüsseln und dann Lösegeld zu fordern: Die Firma Cirosec kämpft auf der guten Seite, sucht bei ihren Kunden nach Schwachstellen und behebt diese. Mehr als 80 Beschäftigte sind für das Unternehmen inzwischen tätig.

Wenn also eine App ein Update fordert, weil eine Sicherheitslücke behoben werden soll, oder wenn in den Nachrichten von Hackern die Rede ist, die solch eine Lücke ausgenutzt haben, dann weiß Strobel, wie so etwas aussieht. „Grundsätzlich handelt es sich um Programmierfehler, Konfigurationsfehler oder Architekturdefizite“, erklärt der Geschäftsführer.

> „Der Klassiker ist heute der Programmierfehler.“
> Stefan Strobel

Architekturfehler heißt dabei aber nicht, dass jemand beim Bau des Firmengebäudes gepfuscht hat. Strobel nennt ein Beispiel: Ein Autohaus hatte auf seinem Server, über den alle Rechner der Standorte liefen, den Zugriff für seinen Internet-Dienstleister offen gelassen. Für den Cirosec-Chef großer Leichtsinn: „Jeder andere kann auch versuchen, sich auf diesem Weg im System anzumelden.“

Zweiter Faktor nötig

Niemals dürfe der Zugang einfach mit Name und Passwort möglich sein, es sei immer ein zweiter Faktor zur Authentifizierung nötig, warnt er. Im konkreten Fall legten Hacker den Server lahm, alles musste mühsam wieder aus Backup-Dateien aufgebaut werden. Diesmal allerdings ohne einfachen Zugang für den IT-Dienstleister.

„Der Klassiker ist heute aber der Programmierfehler“, erläutert der Unternehmer: Programmierer übersehen manchmal, dass sich durch geschicktes Agieren und raffinierte Eingaben das System austricksen lasse. Etwa in Suchanfrage-Feldern: Da werden verschiedene Begriffe normalerweise durch Semikolon abgegrenzt. Wer aber nach einem Begriff inklusive Semikolon suchen lässt, erhält eine weitere Suchoption – und könne dort einen kompletten Softwarebefehl eingeben. „Festplatte verschlüsseln“, zum Beispiel. „Es gibt immer noch Entwickler, die in dieser Angelegenheit nicht richtig geschult sind“, bedauert Strobel.

Solche Fehler sind eher einfach zu finden. Bei anderen hilft inzwischen die KI: Sie kann viel schneller typische Schwachstellen auch in langen Codes ausfindig machen. Fatal sei es etwa, wenn ein Unternehmen nicht die neueste Version seiner Software verwendet. Die alte werde ja aus guten Gründen nicht mehr ausgeliefert – meist, weil ein Fehler vom Hersteller selbst entdeckt wurde. KI könne den alten mit dem aktuellen Code rasch vergleichen, die Unterschiede ausfindig machen und die Lücken angreifen. „Manchmal sind das klitzekleine Fehler – auf die Idee muss man erst mal kommen“, sagt Strobel.

KI kann das. 2025 waren in einer Datenbank für Softwarefehler etwas mehr als 40.000 Schwachstellen aufgeführt – aktuell sind es bereits 35.000 mehr, berichtet er. Das machten sich einige sogar zunutze, um sich etwas hinzuzuverdienen: Sie melden entdeckte Schwachstellen dem Softwarehersteller, der je nach Grad der Gefahr ein „bug bounty“, eine Belohnung für die ehrlichen Finder, ausschüttet – manchmal sogar in fünfstelliger Höhe. Daraus ist mittlerweile ein regelrechter Markt entstanden, mit offiziellen und inoffiziellen Plattformen. „Inzwischen werden die Hersteller mit Meldungen regelrecht überschwemmt“, erzählt der Cirosec-Chef. „Ich hoffe, dass das auch einmal wieder abflaut. Irgendwann dürfte KI ja alle Schwachstellen gefunden haben.“

Quanten-sichere Technologien

Bliebe noch Quantencomputing: Eine Zeit lang hieß es, dass die neuartigen Rechner alle Verschlüsselungen überwinden können. Doch das war einmal – inzwischen gebe es quanten-sichere Technologien, erläutert der Geschäftsführer. Obwohl diese Art von Computern noch kaum verbreitet und lange noch nicht leistungsfähig genug ist, sollten sich Unternehmen darauf einstellen, warnt er. „Solche Projekte haben auch schon begonnen.“

Hacken hat jedenfalls Hochkonjunktur: Vergangenes Jahr waren weltweit mindestens 8100 Firmen, Verwaltungen und Institutionen betroffen, dieses Jahr sind es bereits 7500 – und das letzte Quartal hat gerade erst begonnen. „Es wird nicht weniger. Es flaut nicht ab“, sagt Stefan Strobel. „Aber KI ist auch nicht das Ende der Welt. KI kann nicht alles hacken – und man braucht auch nicht KI, um sich zu schützen.“ Sicherheitsrelevante Betriebe nutzen etwas ganz anderes: das Zwiebelschalen-Prinzip – mehrere Umgebungen, bevor man in den Kern vordringen kann.