FORSCHUNG KOMPAKT

KI hilft bei der Erkennung von Cyberangriffen auf Unternehmensnetze

AMIDES erkennt neue Varianten von Cyberattacken

Cyberangriffe haben sich zu einem großen Risiko für Unternehmen und andere Organisationen entwickelt. Um Datendiebstahl, Sabotage und Erpressung vorzubeugen, nutzen viele Firmen und Behörden deshalb sogenannte Sicherheitsinformations- und Ereignismanagement-Systeme (SIEM), die Cyberattacken mithilfe von Detektionsregeln bzw. Signaturen entdecken können. Forschende des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie FKIE haben jedoch in umfangreichen Tests nachgewiesen, dass Angreifende viele solcher Signaturen leicht umgehen können. Ein neues Open-Source-System des Fraunhofer FKIE soll hier Abhilfe schaffen: Auf Basis von KI erkennt AMIDES Angriffe, die klassische Signaturen übersehen.

Die Bedrohung durch Cyberattacken und Industriespionage hat sich im Jahr 2024 weiter verschärft: Nach Angaben einer Studie des Digitalverbands Bitkom sind acht von zehn Unternehmen in Deutschland bereits Opfer von Datendiebstahl und ähnlichen Angriffen geworden. Der durch Netzwerkeinbrüche entstandene Schaden geht in die Milliarden. Das Problem: Die Angriffsarten und -methoden ändern sich ständig oder werden von den Angreifern geringfügig abgewandelt. Daher werden der Diebstahl und die Manipulation von Daten oftmals erst bemerkt, wenn es zu spät ist.

Open-Source-System erkennt Signatur-Umgehungen durch adaptive Missbrauchserkennung

Bislang basiert die Detektion von Cyberangriffen in Organisationen überwiegend auf Signaturen bzw. Detektionsregeln, die von Sicherheitsexperten auf Basis bereits bekannter Angriffe erstellt wurden. Diese Signaturen sind das Herzstück eines SIEM-Systems. Forschende des Fraunhofer FKIE in Bonn haben jedoch aufgedeckt, dass Angreifende viele solcher Signaturen leicht umgehen können. Zwar lassen sich alternativ auch Detektionsmethoden aus dem Bereich der Anomalie-Erkennung einsetzen, um Angriffe trotz umgangener Signaturen aufzuspüren. Daraus resultieren jedoch häufig viele Fehlalarme, die aufgrund der hohen Anzahl gar nicht alle untersucht werden können. Um dieses Problem zu lösen, haben die Forschenden des Fraunhofer FKIE als praxistauglichen Mittelweg ein System entwickelt, das mithilfe von Machine Learning Angriffe erkennt, die existierenden Signaturen ähnlich sind: Mit AMIDES, kurz für Adaptive Misuse Detection System, führen die Expertinnen und Experten ein Konzept zur adaptiven Missbrauchserkennung ein, das überwachtes Maschinelles Lernen nutzt, um potenzielle

Kontakt
Monika Landgraf | Fraunhofer-Gesellschaft, München | Kommunikation | Telefon +49 89 1205-1333 | presse@zv.fraunhofer.de
Silke Wiesemann | Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE | Telefon +49 228 9435-103 | Fraunhoferstraße 20 | 53343 Wachtberg | www.fkie.fraunhofer.de | silke.wiesemann@fkie.fraunhofer.de

Regelumgehungen zu erkennen und gleichzeitig darauf optimiert ist, Fehlalarme auf ein Minimum zu reduzieren. Die frei verfügbare Open-Source-Software (siehe Link unten) adressiert vor allem größere Organisationen, die bereits über ein zentrales Sicherheitsmonitoring verfügen und dieses verbessern möchten.

»Signaturen sind zwar das wichtigste Mittel, um Cyberangriffe in Unternehmensnetzwerken zu erkennen, sie sind aber kein Allheilmittel«, sagt Rafael Uetz, Wissenschaftler am Fraunhofer FKIE und Leiter der Forschungsgruppe »Intrusion Detection and Analysis«. »Bösartige Tätigkeiten können häufig unerkannt durchgeführt werden, indem der Angriff leicht modifiziert wird. Angreifende versuchen, der Erkennung durch verschiedene Verschleierungstechniken zu entgehen, etwa durch das Einfügen von Dummy-Zeichen in Befehlszeilen. Der Angreifer schreibt den Befehl so, dass die Signatur ihn nicht findet«, erläutert der Forscher das Vorgehen der Cyberkriminellen. An diesem Punkt setzt AMIDES an: Die Software führt eine Merkmalsextraktion auf Daten sicherheitsrelevanter Ereignisse durch, zum Beispiel auf der Befehlszeile neu gestarteter Programme. Mithilfe von Machine Learning werden dann Befehlszeilen erkannt, die denen ähneln, auf die die Detektionsregeln anschlagen, die aber nicht genau diese Signaturen treffen. In diesem Fall würde AMIDES einen Alarm auslösen. Der Ansatz wird als adaptive Missbrauchserkennung bezeichnet, da er sich an die Zielumgebung anpasst, indem er auf ihr Normalverhalten trainiert wird, um potenzielle Angriffe von harmlosen Ereignissen richtig zu unterscheiden.

Adaptive Missbrauchserkennung ermöglicht Regelzuordnungen

Neben der Möglichkeit, bei potenziellen Umgehungen Warnungen auszulösen, bietet der neue Ansatz auch eine Funktionalität, die die Forschenden als Regelzuordnung bezeichnen. Wenn eine herkömmliche Detektionsregel zur Missbrauchserkennung ausgelöst wird, kann ein Analyst diese Regel einfach anzeigen, um herauszufinden, was passiert ist, da Regeln normalerweise einen aussagekräftigen Titel und eine Beschreibung neben den Signaturen enthalten. Vielen auf Maschinellem Lernen basierenden Systemen fehlt dieser Vorteil jedoch, und sie lösen nur eine Warnung ohne weiteren Kontext aus. Da die adaptive Missbrauchserkennung aus SIEM-Detektionsregeln lernt, sind während des Trainings Informationen darüber verfügbar, welche Merkmale in welchen Regeln enthalten sind, sodass AMIDES abschätzen kann, welche Regeln wahrscheinlich umgangen wurden.

Im Rahmen eines umfangreichen Tests mit Echtdaten einer deutschen Behörde konnte AMIDES bereits evaluiert werden. Uetz: »Diese Tests haben gezeigt, dass unsere Lösung das Potenzial hat, die Erkennung von Netzwerkeinbrüchen signifikant zu verbessern.« Mit seiner Standardempfindlichkeit erkannte AMIDES erfolgreich 70 Prozent der Umgehungsversuche ohne Fehlalarme. In puncto Geschwindigkeit zeigten die Messungen, dass das System schnell genug für den Livebetrieb auch in sehr großen Unternehmensnetzen ist.

Download-Link AMIDES:

GitHub - fkie-cad/amides: An Adaptive Misuse Detection System

Abb. 1 Mit AMIDES haben Forschende des Fraunhofer FKIE eine Lösung entwickelt, die das Potenzial hat, die Erkennung von Netzwerkeinbrüchen signifikant zu verbessern.

© Montage: 123RF Galina Peshkova/skorzewiak