FRAUD DETECTION 4.0

Internetbetrüger werden immer gewiefter – also braucht es auch intelligentere Schutzmassnahmen. Dieser Gedanke stand am Anfang eines Machine Learning-Entwicklungsprojekts von Ergon, das inzwischen erste Erfolge aufweist.

→ **VON ADRIAN BERGER**

Der Zahlungsverkehr ist das beliebteste Angriffsziel für Hacker – kein Wunder, ist er doch eine der wichtigsten Anwendungen im Finanzbereich. Hier sitzen Hacker für Manipulationen zu ihren Gunsten direkt an der Quelle. Das Verhindern von Missbrauch gehört darum zu den kritischen Sicherheitsmassnahmen im E-Banking – denn haben Kunden das Vertrauen in ein Institut erst einmal verloren, ist der Schaden immens.

SCHUTZMASSNAHMEN ALS HÜRDE UND KOSTENTREIBER

Zum Erkennen und Verhindern von Missbrauchsversuchen gibt es verschiedene Ansätze. Eine technisch einfache Massnahme ist zum Beispiel, vom Anwender im E-Banking nach dem Login eine zusätzliche Autorisierung pro Transaktion zu verlangen. Das bedeutet, dass er nach einer starken Authentisierung seine Transaktion zusätzlich mit einem Token verifizieren muss. Dieser Schritt ist zwar wirkungsvoll, aber für den Nutzer eine zusätzliche Hürde und dadurch eher wenig kundenfreundlich.

Ein weiterer Ansatz ist es, dass geschultes Personal «manuell» alle getätigten Transaktionen durchgeht und den Kunden zur Bestätigung per Telefon anruft, wenn eine verdächtige Transaktion stattgefunden hat. Diese Massnahme ist für den Anbieter relativ teuer, nicht nur wegen der personellen Ressourcen, sondern auch, weil ein Regelwerk benötigt wird, das definiert, wann eine Transaktion wirklich verdächtig ist und autorisiert werden muss.

Bei den Banken am weitesten verbreitet ist derzeit ein halbautomatisches regelbasiertes System, das evaluiert, welche Zahlungen eine spezielle Autorisierung benötigen (z.B. neuer Empfänger, sehr hoher Geldbetrag, ungewöhnliches Empfängerland etc.). Dank dieser Regeln ist jeder Schritt der Transaktionsautorisierung nachvollziehbar. Der Nachteil ist allerdings, dass das System statisch ist: Neue Angriffsszenarien erfordern Anpassungen im Zahlungsverkehr und damit neue Autorisierungsregeln. Den Überblick über das komplexe Regelwerk haben nur die wenigen Mitarbeitenden, die es pflegen. Das Potential für Fehler und «false positives» steigt, das heisst, es werden zu viele Transaktionen fälschlicherweise als «verdächtig» eingestuft. Die daraus folgenden hohen Interaktionsraten mit den Endkunden durch die Hotline lassen die Kosten steigen.

Fraud Detection in Kombination mit der Airlock Suite

Die Airlock Suite ist ein vorgelagertes Sicherheitssystem bestehend aus einer kombinierten Lösung aus Web Application Firewall und Identity und Access Management. Sie ist die schweizweit am meisten genutzte Security-Lösung für Applikationssicherheit und international bei über 350 Banken, Versicherungen und anderen Organisationen im Einsatz.

«Prevention»-Massnahmen (Airlock Suite)

Bereits auf der Web Application Firewall können Parameter der Laufzeitumgebung wie Browser, Klickverhalten, Malewaredetection oder Bildschirmauflösung aufgezeichnet und überprüft werden. In einem sogenannten Client und Session Fingerprinting werden alle Laufzeitumgebungsparameter geprüft, um Manipulationsversuche innerhalb der Session zu erkennen.

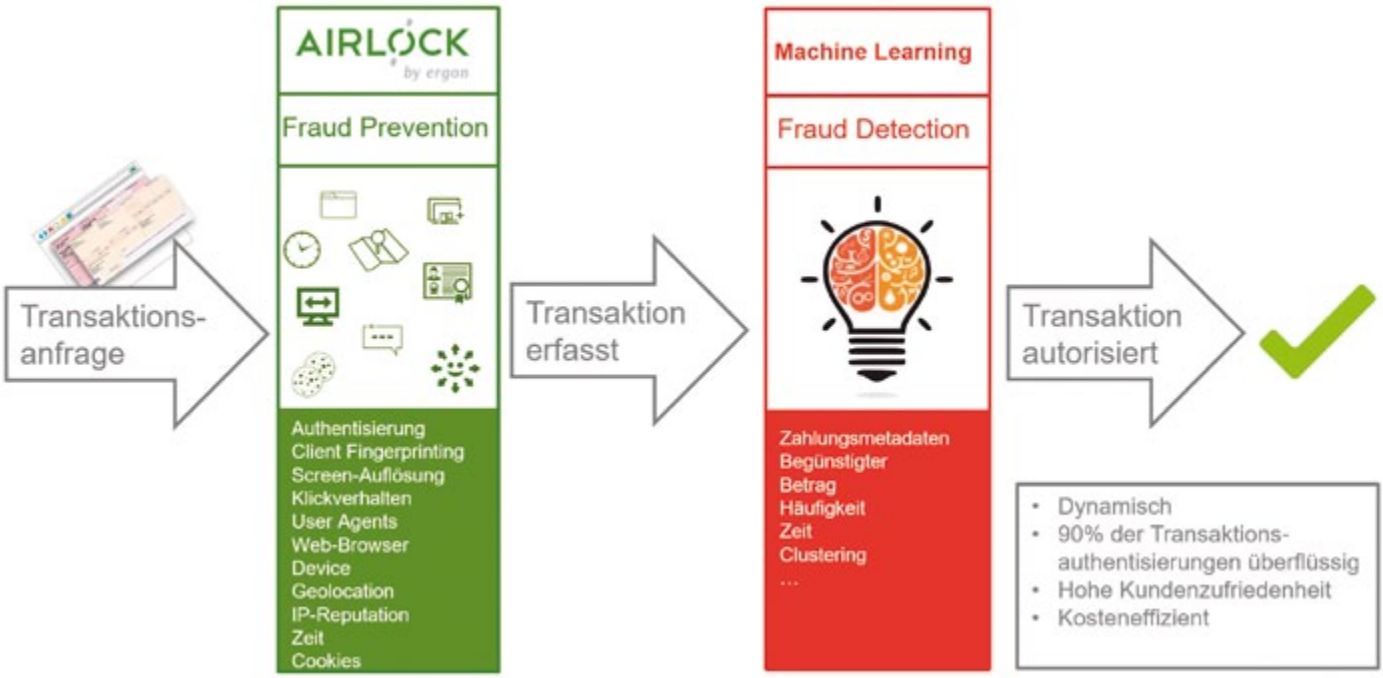
Eine weitere Möglichkeit zur Fraud Detection auf der WAF ist dynamisches Whitelisting oder Dynamic Value Endorsement (DyVE). Ein einfaches Beispiel sind Online-Banking-Transaktionen. Mittels DyVE kann man auf Airlock WAF erzwingen, dass übermittelte Transaktionen lediglich Konten belasten, die vorgängig vom Banking-Server zur Auswahl gestellt wurden.

Ein weiteres Mittel zur Betrugsbekämpfung in der Airlock Suite ist die risikobasierte Authentisierung. Starke Authentisierung mit zwei Faktoren ist heute Standard für geschäftskritische Webanwendungen wie E-Banking. Im täglichen Gebrauch wird diese Sicherheitsmassnahme jedoch von Anwendern oft als mühsam empfunden. Die risikobasierte Authentisierung, auch adaptive Authentisierung genannt, setzt genau hier an. Es wird der Kontext eines Zugriffs genau analysiert und mit vergangenen Sitzungen des gleichen Benutzers verglichen. Kommt Airlock IAM beispielsweise zum Schluss, dass sich der Benutzer von seinem gewohnten Arbeitsplatz im Intranet oder aus seinem Home-Office anmelden möchte, kann auf den zweiten Faktor verzichtet werden. Durch Analyse der Authentisierungshistorie werden Parameter wie die Geolokation, IP Reputation, Zeit, Cookies oder Browser auf das übliche Verhalten der Identität geprüft.

«Detection»-Massnahmen (Machine Learning)

Nachgelagert zum Schutz durch die Airlock Suite bietet Fraud Detection mit Machine Learning einen Schutz, der innerhalb der Applikation greift, wenn ein Betrüger trotz der anderen Sicherheitsmassnahmen bis ins System eindringen konnte. Hier können Empfänger, Metadaten der Zahlung, Beträge, Frequenz und andere Parameter geprüft werden, um Betrugsversuche zuverlässig und automatisiert zu erkennen. Das Machine Learning als Kombination mit der Airlock Suite ist sinnvoll, weil es gezielt auf Betrugserkennung fokussiert, wohingegen die Airlock Suite selbst die Applikationssicherheit zum Ziel hat.

www.airlock.com



SCHNELL AUF NEUE BEDROHUNGEN REAGIEREN

Schon heute zeichnet zudem sich ab, dass bei den neuartigen Bedrohungslagen und immer professioneller organisierten Betrügern auch halbautomatisierte Systeme für guten Schutz nicht mehr ausreichend sind. Dies hat die Securityabteilung von Ergon dazu bewogen, ein neues Verfahren zu entwickeln und zu testen: Eine intelligente Fraud Detection mithilfe von Machine Learning. Die Idee war, ein selbstlernendes System zu schaffen, das besser und schneller als menschliche Experten mit grossen Datenmengen umgehen kann und Fehler und Betrugsversuche zuverlässig aufspürt. Durch das Erkennen und Verallgemeinern von Mustern und Gesetzmässigkeiten soll es grosse Mengen unbekannter Daten analysieren, richtig bewerten und dazulernen, ohne dass manuell neue Regeln definiert werden oder andere Interaktionen stattfinden müssen.

PILOTVERSUCH ZEIGT ERSTE RESULTATE

Was brauchte es für dieses Projekt? Zuerst einmal viele Daten aus dem Zahlungsverkehr, Wissen im Bereich Data Science, ein ausgeprägtes Domänenwissen im Finanzbereich - und dazu einen experimentierfreudigen Kunden, der bereit war, hochsensible Daten zur Verfügung zu stellen. Dieser war schnell gefunden und das Projekt mit Forschungscharakter konnte gestartet werden.

In einem ersten Schritt wurde ein System entwickelt, das mittels Data Mining aus einer Teilmenge von 10.000 Zahlungen als Lerndaten Muster und Gesetzmässigkeiten lernen und Betrugsversuche aufspüren sollte. Dann wurde der «Lernerfolg» des Fraud Detection-Systems überprüft: 300 weitere Transaktionen wurden von menschlichen Experten mit bestehenden Methoden bewertet und parallel vom neu entwickelten System analysiert. Das Resultat war beeindruckend: Bereits im ersten Versuch lieferte das selbstlernende System zuverlässigere Ergebnisse bei der Betrugserkennung als die menschliche Expertengruppe.

Nun soll das Konzept weiter verbessert werden, damit es noch genauere Ergebnisse liefert. Dafür sind, wie für Machine Learning üblich, mehr Daten auch von anderen Systemen erforderlich, denn je mehr Lerndaten dem System «gefüttert» werden können, umso intelligenter wird es. Die aktuellen Forschungsarbeiten sind jetzt in vollem Gange. Es werden bereits Verknüpfung mit anderen Transaktionssystemen erstellt, um mehr Daten zu erhalten und dynamisch reagieren zu können.

Das Ziel der Lösung ist es, Transaktionen benutzerfreundlicher zu machen: Durch maschinelles Wissen und intelligente, verknüpfte Systeme werden die aktuell mehr als 90% offensichtlich überflüssigen Transaktionsautorisierungen obsolet.

Für einen möglichst umfassenden Schutz vor Betrug sollte Machine Learning zusammen mit anderen Verfahren angewendet werden. Ergon wird die Fraud Detection-Lösung künftig in Kombination mit der Airlock Suite anbieten und somit das Zusammenspiel von «Prevention»- und «Detection»-Mechanismen ermöglichen. Durch diesen gesamtheitlichen Ansatz kann Betrugserkennung im Zahlungsverkehr zuverlässig mit einer minimalen False-Positive-Rate umgesetzt werden. Die Kosten für Fraud Detection werden reduziert und weniger manuelle Interaktion wird erforderlich. ←

Zum Autor

Adrian Berger ist Dipl. Informatikingenieur ETH und Managing Director Finance Solutions bei Ergon Informatik AG

Zum Unternehmen:
Die 1984 gegründete Ergon Informatik AG ist führend in der Herstellung von individuellen Softwarelösungen und Softwareprodukten. 260 hoch qualifizierte IT-Spezialisten antizipieren dank herausragendem Know-how neue Technologietrends und stellen mit innovativen Lösungen Wettbewerbsvorteile sicher. Neben der international erfolgreichen Security-Software Airlock Suite realisiert Ergon hauptsächlich Grossprojekte im B2B-Bereich.

Mehr Informationen:
www.ergon.ch

ergon
smart people – smart software