Eintrittsgenehmigung mit Hirnschmalz – IAM-Lösungen brauchen Intelligenz

Vor einiger Zeit tauchte KI noch als wiederbelebtes Buzzword auf. Mittlerweile ist sie durch diverse wissenschaftliche Durchbrüche für viele Branchen die De-facto-Zukunft geworden. Hersteller von Sicherheitslösungen sind nun in Zugzwang und sollten nochmals die Ausrichtung ihrer Produktentwicklung überdenken.

Die Cyber Grand Challenge (CGC) der DARPA hat 2016 einen Meilenstein des Hackings hervorgebracht: Vollautomatisierte Systeme suchten Sicherheitslücken des Gegners, um diese zu attackieren. Zudem patchten sie in der gleichen Zeit die eigenen, um mögliche Angriffe abzuwehren. Das Challenge-Team «Shellphish» veröffentlichte im Nachgang den Quellcode seines sogenannten «Mechanical Phish», beschrieb dessen Aufbau und Strategie.

Was dabei wie ein Streifen aus dem Science-Fiction-Genre klingt, ist heute zum Greifen nahe. Viele Unternehmen tüfteln bereits länger an der künstlichen Intelligenz (KI), investierten kräftig in den anfänglichen Hype und meldeten mehrfache Erfolge beim Überwinden wissenschaftlicher Hürden. Dabei ist der Traum, Maschinen eine gewisse «Seele» zu verleihen nicht einmal neu: Game-Hersteller für PCs und Konsolen setzen seit Jahrzehnten sogenannte KI-Engines für ihre Strategiespiele ein, nur galt diese Technik bisher als eingeschränkt.

Die prominentesten Unternehmen, die sich heute intensiv mit KI beschäftigen, stammen längst nicht mehr aus der Gaming-Branche. Inzwischen berichten fast alle Medien über Projekte aus dem Hause Google, Amazon oder Microsoft. Auch die Autoindustrie investiert massiv in die zukünftige Mobilität mit KI. Der ursprüngliche Treiber dürfte jedoch weiterhin die Verteidigungsindustrie sein. Neben

DARPA sind viele Rüstungsunternehmen weltweit mit im Boot, etwa für die Entwicklung der Robotik und intelligenter, unbemannter Waffensysteme. Nicht zuletzt ebnete Big Data die notwendige Datenbasis für das sogenannte Deep Learning.

Meilenstein in der IT-Security

Die vom Team «Shellphish» entwickelten intelligenten Angriffs-, Abwehr- und Heilmechanismen sind ein Meilenstein in der IT-Security. Die Opfer von Cyberattacken könnten die Technologie als neue Verteidigungsstrategie einsetzen. Und die nächste Hacker-Generation könnte die KI dafür verwenden, um Angriffe zu lancieren – ob sie nun staatlicher oder privater Natur sind.

Breit gefächerte, intelligent automatisierte Angriffsszenarien zeigen, dass es in naher Zukunft nicht mehr ausreichen wird, statisch verdrahtete Abwehrmechanismen zu implementieren. Hersteller von IAM-Lösungen müssen daher ebenfalls im Rahmen von «Threat Intelligence» reagieren. So wird es etwa notwendig sein, bei einer regulären Legitimation eines Benutzers sein bisheriges Nutzungsverhalten im Vorfeld zu analysieren. Konkret könnte ein IAM dann intelligent entscheiden, ob es einen Benutzer mit gültigen «Credentials» über eine VPN-Leitung passieren lässt – obwohl dieser sich zuvor noch nie über eine VPN-Leitung angemeldet hat –, oder ihn in eine Quarantäne mit eingeschränkten Rechten stellt. Ein anderes Anwendungsbeispiel könnte sein, dass die intelligente IAM-Lösung eine mögliche «Priviledge Escalation» mithilfe von KI gestützten Verhaltens- und Zeitreihenanalysen in Kombination mit Organisations- und Freigabeprozessen erkennt und zuständige Instanzen automatisch warnt. Die Ergebnisse nutzt die Lösung wiederum als weitere Basis des Lernprozesses.

Es zeichnet sich also immer mehr ab, dass sich auch Hersteller von Sicherheitslösungen mit dem Thema intensiver befassen und in Verbindung mit der rasant voranschreitenden KI bereits jetzt die mögliche Integration in Betracht ziehen müssen. Andernfalls ist die Gefahr gross, dass ihre Produkte später wie ein Oldtimer in der Autogalerie stehen werden: Top in Schuss, doch mit überholter Technik ein Staubfänger.

DER AUTOR

Orkan Yoksulabakan
Managing Consultant IT-Security, ITSENSE